Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	AMBIENTE
SERVIZIO: denominazione e punti di contatto	AMBIENTE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Interventi per il contrasto del randagismo

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	AMBIENTE
SERVIZIO: denominazione e punti di contatto	AMBIENTE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Contributi per attivita' ambientali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	AMBIENTE
SERVIZIO: denominazione e punti di contatto	AMBIENTE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Mantova Ambiente S.r.l

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo tassa sui rifiuti TARES/TARI

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	AMBIENTE
SERVIZIO: denominazione e punti di contatto	AMBIENTE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	Mantova Ambiente S.r.l

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Affidamento appalto di lavori, servizi e forniture di importo inferiore a 40.000 euro tramite il sistema dell'affidamento diretto

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Anziani ed adulti con disagio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assistenza domiciliare
Pasti a domicilio

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Anziani ed adulti con disagio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	Fondazione Contessa Rizzini Villa Oleandri Fondazione Mons. Arrigo Mazzali

contatto	Casa riposo Ducale - Societa' Dolce Congregazione Povere Figlie di Maria SS Incoronata Ospedale Civile Gonzaga Fondazione Boni Casa Di Riposo Villa Azzurra Gruppo Gheron - RSA Villa Carpaneda Istituto Bassano Cremonesini Il Sorriso srl -Rsa Beata Paola I Tulipani s.r.l. Citta' delle Persone - casa residenza anziani I Girasoli Fondazione Grimani Buttari Fondazione Tosi Cippelletti Fondazione Antonio Nuvolari Fondazioen Salutevita Onlus - Casa Canossa Fondazione Casa Leandra Fondazione Baguzzi Dassu' Coop sicalie SAI - RSA Casa Pace di Mantova Coop La Provvidenza - Villa Aurelia - unita' di San Michele in Bosco (MN) A.S.P. e F. Azienda Servizi alla Persona e alla Famiglia
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione

	misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC

	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici

	possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o

	programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che

	trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi

	- MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Inserimenti in strutture
Integrazione rette case di riposo
Servizio RSA e riabilitazione

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 13 - Servizi sociali - Trattamento di dati relativi all'attivita' ricreative per la promozione del benessere della persona e della comunita', per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Anziani ed adulti con disagio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Teleassistenza
Sportello Alzheimer

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Anziani ed adulti con disagio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Contributi economici
Carta per ottenere agevolazioni presso gli esercizi commerciali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 15 - Servizi sociali - Trattamento di dati relativi all'attivita' di gestione dell'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Anziani ed adulti con disagio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	Fondazione Contessa Rizzini Villa Oleandri Fondazione Mons. Arrigo Mazzali

contatto	Casa riposo Ducale - Societa' Dolce Congregazione Povere Figlie di Maria SS Incoronata Ospedale Civile Gonzaga Fondazione Boni Casa Di Riposo Villa Azzurra Gruppo Gheron - RSA Villa Carpaneda Istituto Bassano Cremonesini Il Sorriso srl -Rsa Beata Paola I Tulipani s.r.l. Citta' delle Persone - casa residenza anziani I Girasoli Fondazione Grimani Buttari Fondazione Tosi Cippelletti Fondazione Antonio Nuvolari Fondazioen Salutevita Onlus - Casa Canossa Fondazione Casa Leandra Fondazione Baguzzi Dassu' Coop sicalie SAI - RSA Casa Pace di Mantova Coop La Provvidenza - Villa Aurelia - unita' di San Michele in Bosco (MN) A.S.P. e F. Azienda Servizi alla Persona e alla Famiglia
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione

	misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC

	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici

	possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o

	programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che

	trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi

	- MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Centri sociali per anziani

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Anziani ed adulti con disagio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Soc. coop La Dolce C.H.V. - COOPERATIVA SOCIALE DI SOLIDARIETA' A RESPONSABILITA' LIMITATA - ONLUS SOL.CO. TRASPORTI - Societa' Cooperativa Onlus

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio di trasporto anziani

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Anziani ed adulti con disagio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Procedure correlate alla nomina amministratore di sostegno, interdizione o inabilitazione (su richiesta dell'autorita' giudiziaria)
Amministrazione di sostegno

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Anziani ed adulti con disagio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	Fondazione Contessa Rizzini Villa Oleandri

denominazione e punti di contatto	Fondazione Mons. Arrigo Mazzali Casa riposo Ducale - Societa' Dolce Congregazione Povere Figlie di Maria SS Incoronata Ospedale Civile Gonzaga Fondazione Boni Casa Di Riposo Villa Azzurra Gruppo Gheron - RSA Villa Carpaneda Istituto Bassano Cremonesini Il Sorriso srl -Rsa Beata Paola I Tulipani s.r.l. Citta' delle Persone - casa residenza anziani I Girasoli Fondazione Grimani Buttari Fondazione Tosi Cippelletti Fondazione Antonio Nuvolari Fondazioen Salutevita Onlus - Casa Canossa Fondazione Casa Leandra Fondazione Baguzzi Dassu' Coop sicalie SAI - RSA Casa Pace di Mantova Coop La Provvidenza - Villa Aurelia - unita' di San Michele in Bosco (MN) A.S.P. e F. Azienda Servizi alla Persona e alla Famiglia
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza

	inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5

	(CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento

	dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle

	variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia'

	con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative

	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati

	(data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI

ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Convenzioni con Centri di socializzazione

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 21 - Istruzione e cultura - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie
AREA	Area Servizi ai cittadini
SETTORE	SERVIZI EDUCATIVI E PUBBLICA ISTRUZIONE
SERVIZIO: denominazione e punti di contatto	Asilo Nido
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	COOPERATIVA IL GIARDINO DEI BIMBI
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Collocazione fasce tariffarie I.S.E.E. per utenti asilo nido
Iscrizioni e graduatorie per asilo nido

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 23 - Istruzione e cultura - Trattamento di dati relativi alla gestione delle biblioteche e dei centri di documentazione
AREA	AREA SERVIZI GENERALI
SETTORE	CULTURA, TURISMO E PROMOZIONE DELLA CITTA'
SERVIZIO: denominazione e punti di contatto	Biblioteca
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	Internavigare srl

trattamento: denominazione e punti di contatto	Lombardia Informatica SpA EURO E PROMOS Coop. Sociale Le Pagine Charta Cooperativa Sociale Onlus
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Prestito locale
Prestito interbibliotecario
Assistenza alla ricerca

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	Consiglio comunale e commissioni consiliari
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Istituzione commissioni permanenti, temporanee o speciali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	Consiglio comunale e commissioni consiliari
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Procedure di valutazione relative alla verifica dell'impatto della regolamentazione (VIR) ai sensi dell'art. 14, comma 4, della legge 28 novembre 2005, n. 246
Procedure di valutazione relative all'analisi dell'impatto della regolamentazione (AIR) ai sensi dell'art.14, comma 1, della legge 28 novembre 2005, n. 246
Mozioni, ordini del giorno, risoluzioni, interrogazioni ed interpellanze

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	DEMOGRAFICI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Ispettorato Nazionale Lavoro (Mantova) ALER BRESCIA-CREMONA MANTOVA CAMERA COMMERCIO MANTOVA UNEP TRIBUNALE DI MANTOVA

	TEA MANTOVA AMBIENTE TEA SERVIZI CIMITERIALI SORIT SPA Raggruppamento Operativo Speciale (Brescia) QUESTURA DI MANTOVA PROCURA DI MANTOVA POLIZIA DI STATO ASST MANTOVA ISTITUTO COMPRENSIVO MANTOVA 3 ISTITUTO COMPRENSIVO MANTOVA 1 INPS MANTOVA GUARDIA DI FINANZA MANTOVA ARMA DEI CARABINIERI (CC MANTOVA) Aster srl - Agenzia Servizi al Territorio
Responsabile trattamento: denominazione e punti di contatto	Maggioli Spa ASSOCIAZIONE CLUB VIRGILIANO
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4

	(CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza

	con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con

	violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della

	vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito

	sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e

	aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza

	dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Anagrafe: Comunicazioni Prefettura
Anagrafe: Comunicazioni all'ufficio tributi
Anagrafe: Certificati anagrafici
Anagrafe: Variazioni anagrafiche AIRE (Anagrafe Italiani Residenti all'Estero)

Anagrafe: Iscrizione AIRE (Anagrafe Italiani Residenti all'Estero) dei cittadini italiani per trasferimento da AIRE o APR di altro Comune
Anagrafe: Ripristino immigrazione
Anagrafe: Verifica dichiarazione di rinnovo della dimora abituale
Anagrafe: Attestazione di regolarita' di soggiorno
Anagrafe: Attestazione di soggiorno permanente
Anagrafe: Rilascio carta di identita'
Anagrafe: Autentica di firma
Anagrafe: Autentica di copia
Anagrafe: Cancellazione anagrafiche AIRE (Anagrafe Italiani Residenti all'Estero)
Anagrafe: Certificati anagrafici storici
Registro convivenze di fatto
Anagrafe: Iscrizioni registri anagrafici
Anagrafe: Cancellazioni registri anagrafici per irreperibilita'
Anagrafe: Adeguamento anagrafe ai risultati del censimento
Toponomastica: Attribuzione numero civico
Toponomastica: Denominazione nuove strade e piazze
Anagrafe: Variazione di indirizzo

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	DEMOGRAFICI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Ispettorato Nazionale Lavoro (Mantova) ALER BRESCIA-CREMONA MANTOVA CAMERA COMMERCIO MANTOVA UNEP TRIBUNALE DI MANTOVA TEA MANTOVA AMBIENTE

	TEA SERVIZI CIMITERIALI SORIT SPA Raggruppamento Operativo Speciale (Brescia) QUESTURA DI MANTOVA PROCURA DI MANTOVA POLIZIA DI STATO ASST MANTOVA ISTITUTO COMPRENSIVO MANTOVA 3 ISTITUTO COMPRENSIVO MANTOVA 1 INPS MANTOVA GUARDIA DI FINANZA MANTOVA ARMA DEI CARABINIERI (CC MANTOVA) Aster srl - Agenzia Servizi al Territorio
Responsabile trattamento: denominazione e punti di contatto	Maggioli Spa ASSOCIAZIONE CLUB VIRGILIANO
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

	VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI

	PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni

	- MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante

	- MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Anagrafe: Tenuta registro unioni civili
Anagrafe: Accettazione e tenuta dichiarazioni di testamento biologico
Accertamento requisiti di dimora abituale delle variazioni di residenza
Stato civile: Acquisizione della cittadinanza italiana per riconoscimento o dichiarazione giudiziale della filiazione durante la minore eta' del figlio, o nel caso in cui la paternita' o maternita' non puo' essere

dichiarata, purche' sia stato riconosciuto giudizialmente il diritto al mantenimento o agli alimenti, di minore straniero
Stato civile: Acquisizione della cittadinanza italiana per riconoscimento o dichiarazione giudiziale della filiazione o nel caso in cui la paternita' o maternita' non puo' essere dichiarata, purche' sia stato riconosciuto giudizialmente il diritto al mantenimento o agli alimenti, di maggiorenne straniero
Stato civile: Acquisto della cittadinanza per matrimonio
Stato civile: Tutela/Curatela
Stato civile: Trascrizione atti di nascita formati all'estero
Stato civile: Trasmissioni alla Procura della Repubblica
Stato civile: Comunicazioni all'Ufficio anagrafe
Stato civile: Celebrazioni matrimoni civili
Stato civile: Pubblicazioni di matrimonio
Stato civile: Affiliazioni
Stato civile: Disconoscimenti
Stato civile: Riconoscimenti
Stato civile: Annotazione sentenza di rettificazione attribuzione di sesso
Stato civile: Annotazione sentenze di scioglimento del matrimonio civile, di cessazione degli effetti civili del matrimonio religioso (concordatario) o di delibazione sentenze ecclesiastiche di annullamento di matrimonio pronunciate in Italia, provenienti da altri comuni
Separazione consensuale, divorzio congiunto e modifica delle condizioni di separazione o di divorzio innanzi all'Ufficiale di Stato Civile
Stato Civile: Trascrizione atto di matrimonio celebrato all'estero
Stato civile: Adozione
Stato civile: Trascrizione atti di nascita rese dalla Direzione Sanitaria
Stato civile: Redazione atto di nascita
Stato civile: Trascrizione atto di nascita neo-cittadino
Stato civile: Trascrizione atto di matrimonio celebrato in altro comune italiano
Stato Civile: Trascrizione atto di matrimonio concordatario
Stato civile: Redazione atto di morte
Stato civile: Trascrizione atto di morte avvenuta all'estero
Stato civile: Trascrizione atto di morte pervenuto da altro Comune
Stato Civile: Rilascio passaporto mortuario
Stato civile: Cambio nome/cognome

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	DEMOGRAFICI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Ispettorato Nazionale Lavoro (Mantova) ALER BRESCIA-CREMONA MANTOVA CAMERA COMMERCIO MANTOVA UNEP TRIBUNALE DI MANTOVA TEA MANTOVA AMBIENTE

	TEA SERVIZI CIMITERIALI SORIT SPA Raggruppamento Operativo Speciale (Brescia) QUESTURA DI MANTOVA PROCURA DI MANTOVA POLIZIA DI STATO ASST MANTOVA ISTITUTO COMPRENSIVO MANTOVA 3 ISTITUTO COMPRENSIVO MANTOVA 1 INPS MANTOVA GUARDIA DI FINANZA MANTOVA ARMA DEI CARABINIERI (CC MANTOVA) Aster srl - Agenzia Servizi al Territorio
Responsabile trattamento: denominazione e punti di contatto	Maggioli Spa ASSOCIAZIONE CLUB VIRGILIANO
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

	VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI

	PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni

	- MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante

	- MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Elettorale: supporto commissioni elettorali
Elettorale: autorizzazione al voto fuori sezione
Elettorale: voto domiciliare
Elettorale: voto assistito
Elettorale: rilascio tessera elettorale

Elettorale: revisione semestrale liste elettorali
Elettorale: revisione dinamica liste elettorali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	DEMOGRAFICI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Ispettorato Nazionale Lavoro (Mantova) ALER BRESCIA-CREMONA MANTOVA CAMERA COMMERCIO MANTOVA UNEP TRIBUNALE DI MANTOVA TEA MANTOVA AMBIENTE

	TEA SERVIZI CIMITERIALI SORIT SPA Raggruppamento Operativo Speciale (Brescia) QUESTURA DI MANTOVA PROCURA DI MANTOVA POLIZIA DI STATO ASST MANTOVA ISTITUTO COMPRENSIVO MANTOVA 3 ISTITUTO COMPRENSIVO MANTOVA 1 INPS MANTOVA GUARDIA DI FINANZA MANTOVA ARMA DEI CARABINIERI (CC MANTOVA) Aster srl - Agenzia Servizi al Territorio
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

	VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI

	PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni

	- MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante

	- MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Elettorale: iscrizione nell'albo degli scrutatori
Elettorale: aggiornamento albo scrutatori
Elettorale: aggiornamento albo Presidenti di seggio
Elettorale: iscrizione nell'albo dei Presidenti di seggio

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	DEMOGRAFICI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Ispettorato Nazionale Lavoro (Mantova) ALER BRESCIA-CREMONA MANTOVA CAMERA COMMERCIO MANTOVA UNEP TRIBUNALE DI MANTOVA

	TEA MANTOVA AMBIENTE TEA SERVIZI CIMITERIALI SORIT SPA Raggruppamento Operativo Speciale (Brescia) QUESTURA DI MANTOVA PROCURA DI MANTOVA POLIZIA DI STATO ASST MANTOVA ISTITUTO COMPRENSIVO MANTOVA 3 ISTITUTO COMPRENSIVO MANTOVA 1 INPS MANTOVA GUARDIA DI FINANZA MANTOVA ARMA DEI CARABINIERI (CC MANTOVA) Aster srl - Agenzia Servizi al Territorio
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4

	(CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza

	con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con

	violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della

	vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito

	sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e

	aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza

	dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Elettorale: aggiornamento albo Giudici Popolari
Elettorale: iscrizione nell'albo dei Giudici Popolari

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 08 - Servizi demografici/Leva - Trattamento di dati relativi all'attivita' di tenuta del servizio civile
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	DEMOGRAFICI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Registro del servizio civile

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 09 - Servizi demografici/Leva - Trattamento di dati relativi all'attivita' di tenuta delle liste di leva e dei registri matricolari
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	DEMOGRAFICI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Ispettorato Nazionale Lavoro (Mantova) ALER BRESCIA-CREMONA MANTOVA CAMERA COMMERCIO MANTOVA UNEP TRIBUNALE DI MANTOVA TEA MANTOVA AMBIENTE

	TEA SERVIZI CIMITERIALI SORIT SPA Raggruppamento Operativo Speciale (Brescia) QUESTURA DI MANTOVA PROCURA DI MANTOVA POLIZIA DI STATO ASST MANTOVA ISTITUTO COMPRENSIVO MANTOVA 3 ISTITUTO COMPRENSIVO MANTOVA 1 INPS MANTOVA GUARDIA DI FINANZA MANTOVA ARMA DEI CARABINIERI (CC MANTOVA) Aster srl - Agenzia Servizi al Territorio
Responsabile trattamento: denominazione e punti di contatto	Maggioli Spa ASSOCIAZIONE CLUB VIRGILIANO
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

	VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI

	PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni

	- MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante

	- MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Leva: Variazioni liste di leva
Leva: Certificati di leva

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	DEMOGRAFICI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Ispettorato Nazionale Lavoro (Mantova) ALER BRESCIA-CREMONA MANTOVA CAMERA COMMERCIO MANTOVA UNEP TRIBUNALE DI MANTOVA TEA MANTOVA AMBIENTE

	TEA SERVIZI CIMITERIALI SORIT SPA Raggruppamento Operativo Speciale (Brescia) QUESTURA DI MANTOVA PROCURA DI MANTOVA POLIZIA DI STATO ASST MANTOVA ISTITUTO COMPRENSIVO MANTOVA 3 ISTITUTO COMPRENSIVO MANTOVA 1 INPS MANTOVA GUARDIA DI FINANZA MANTOVA ARMA DEI CARABINIERI (CC MANTOVA) Aster srl - Agenzia Servizi al Territorio
Responsabile trattamento: denominazione e punti di contatto	Maggioli Spa ASSOCIAZIONE CLUB VIRGILIANO
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

	VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA

	(Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI

	PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni

	- MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante

	- MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento requisiti di dimora abituale delle variazioni di residenza

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	Edilizia Privata
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate

	dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sanzioni per interventi eseguiti in assenza o difformita' dalla segnalazione certificata di inizio attivita'

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	Edilizia Privata
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per

	favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Restituzione del contributo di costruzione

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
AREA	AREA SERVIZI GENERALI
SETTORE	CULTURA, TURISMO E PROMOZIONE DELLA CITTA'
SERVIZIO: denominazione e punti di contatto	EVENTI CULTURALI E TURISMO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Contributi per manifestazioni
Sovvenzioni e sussidi a sostegno di operatori del settore artistico e culturale

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico
AREA	AREA SERVIZI GENERALI
SETTORE	CULTURA, TURISMO E PROMOZIONE DELLA CITTA'
SERVIZIO: denominazione e punti di contatto	EVENTI CULTURALI E TURISMO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	S.c.r.l. VERONA 83
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Organizzazione manifestazioni

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Famiglie
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Buono casa

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 17 - Servizi sociali - Trattamento di dati relativi all'attivita' di prevenzione e sostegno alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno) e centri documentali (per prevenzione)
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Famiglie
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sostegno all'Inclusione Attiva (SIA)

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	GIUNTA COMUNALE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomine e affidamenti incarichi per prestazioni o servizi per i quali le determinazioni siano fondate su rapporti fiduciari

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	GIUNTA COMUNALE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessioni discrezionali non vincolate di contributi, benefici, esoneri e sovvenzioni (Provvedimenti amministrativi discrezionali nell'an e nel contenuto)

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	GIUNTA COMUNALE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il

	riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Lasciti e donazioni

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	GIUNTA COMUNALE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Convenzioni con associazioni e altri enti di diritto privato non di competenza del Consiglio

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	TERRITORIO E LAVORI PUBBLICI
SERVIZIO: denominazione e punti di contatto	Manutenzioni
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Pronta reperibilita'

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	TERRITORIO E LAVORI PUBBLICI
SERVIZIO: denominazione e punti di contatto	Manutenzioni
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sopralluogo

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Minori e persone diversamente abili
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Gruppo Gamma societa' coopertiva Soc. Coop. La Quercia onuls Alce Nero Soc. coop onlus Caritas Mantova- Associaione AGAPE Aster srl - Agenzia Servizi al Territorio

	SOL_CO MANTOVA Cooperativa La Stazione Fior di loto soc. coop. Sociale onlus
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure

	minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione)

accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo

	dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente

Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs.

	196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al

	fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio assistenza domiciliare minori

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Minori e persone diversamente abili
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Fior di loto soc. coop. Sociale onlus

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Ricovero minori in struttura

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Minori e persone diversamente abili
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	ANFFAS Onlus Mantova Soc. coop La Dolce C.S.A. Cooperativa servizi assistenziali C.H.V. - COOPERATIVA SOCIALE DI SOLIDARIETA' A

	RESPONSABILITA' LIMITATA - ONLUS SOL.CO. TRASPORTI - Societa' Cooperativa Onlus Gruppo Gamma societa' coopertiva Cooperativa Sociale Minerva Soc. Coop. La Quercia onuls Alce Nero Soc. coop onlus Speranza soc. coop. Sociale onlus SOL_CO MANTOVA Cooperativa La Stazione Fior di loto soc. coop. Sociale onlus
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non

	autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle

	specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore:

	regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

	- MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del

	trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali

	- MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assistenza alloggiati temporanea
Affidamento familiare
Progetti minori in carico

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	TERRITORIO E LAVORI PUBBLICI
SERVIZIO: denominazione e punti di contatto	Opere e Lavori pubblici
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Varianti in corso d'opera lavori in appalto

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	TERRITORIO E LAVORI PUBBLICI
SERVIZIO: denominazione e punti di contatto	Opere e Lavori pubblici
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Liquidazioni acconti o rata di saldo e omologa del certificato di regolare esecuzione per contratti pubblici di lavori, servizi e forniture in economia
Coordinatore della sicurezza in fase di progettazione
Affidamento direzione lavori in appalto a professionisti esterni
Alta sorveglianza lavori eseguiti in project financing o in convenzione con altri soggetti terzi
Partecipazione a commissioni di collaudo
Affidamento incarico esterno di coordinatore della sicurezza
Affidamento progettazione a professionisti esterni
Direzione lavori
Collaudo
Subappalto
Redazione cronoprogramma

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 11 - Servizi sociali - Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale
AREA	Area Servizi ai cittadini
SETTORE	SERVIZI EDUCATIVI E PUBBLICA ISTRUZIONE
SERVIZIO: denominazione e punti di contatto	Piano diritto allo Studio e programmazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	C.S.A. Cooperativa servizi assistenziali

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assistenza educativa alunni disabili in ambito scolastico

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)
AREA	Area Servizi ai cittadini
SETTORE	SERVIZI EDUCATIVI E PUBBLICA ISTRUZIONE
SERVIZIO: denominazione e punti di contatto	Piano diritto allo Studio e programmazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	C.S.A. Cooperativa servizi assistenziali
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Testi scolastici per alunni della scuola primaria
Gestione tariffe e rette
Prestazioni agevolate (servizi educativi, socio-assistenziali, etc.)

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 22 - Istruzione e cultura - Trattamento di dati relativi relativi all'attivita' di formazione ed in favore del diritto allo studio
AREA	Area Servizi ai cittadini
SETTORE	SERVIZI EDUCATIVI E PUBBLICA ISTRUZIONE
SERVIZIO: denominazione e punti di contatto	Piano diritto allo Studio e programmazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento:	C.S.A. Cooperativa servizi assistenziali

denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati

	esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti

	necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di

	accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati

	- MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015

	- DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Centro ricreativo estivo - CRE

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
AREA	Area Servizi ai cittadini
SETTORE	SERVIZI EDUCATIVI E PUBBLICA ISTRUZIONE
SERVIZIO: denominazione e punti di contatto	Piano diritto allo Studio e programmazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Contributo a istituti scolastici paritari
Contributo regionale Buono-libri

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	Area Servizi ai cittadini
SETTORE	SERVIZI EDUCATIVI E PUBBLICA ISTRUZIONE
SERVIZIO: denominazione e punti di contatto	Piano diritto allo Studio e programmazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	CIR FOOD s.c.
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio pre e post scuola
Servizio di ristorazione scolastica

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia giudiziaria
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Trasmissione notizie di reato all'A.G.
Indagini su delega Procura

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia locale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	Maggioli Spa

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Geolocalizzazione delle autovetture di servizio

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia locale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	Aster srl - Agenzia Servizi al Territorio

contatto	
Responsabile trattamento: denominazione e punti di contatto	KAPSCH TRAFFICCOM SRL Maggioli Spa
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Contrassegni

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia locale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Aster srl - Agenzia Servizi al Territorio
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rinvenimento oggetti smarriti
Cooperazione con altre forze dell'ordine
Assistenza organi istituzionali: Servizio ordine consiglio comunale
Servizi rappresentanza in celebrazioni e manifestazioni
Recupero veicoli abbandonati su area pubblica
Recupero veicolo rubati trovati in sosta
Videosorveglianza
Accesso alle immagini di videosorveglianza

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia locale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	B.M. servizi srl Project Automation spa Kapsch TrafficCom Srl ANTARES ELETTRONICA SRL Maggioli Spa
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento requisiti di dimora abituale delle variazioni di residenza

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia locale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	Aster srl - Agenzia Servizi al Territorio

Responsabile trattamento: denominazione e punti di contatto	Maggioli Spa
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento requisiti di dimora abituale delle variazioni di residenza
Interventi per manifestazioni, feste, processioni, mercati e manifestazioni sportive
Servizi per obiettivi sensibili
Servizi antiprostituzione
Avvisi di accertamento violazione
Emissioni ruoli riscossione sanzioni
Controllo - Ispezione

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 24 - Polizia municipale - Trattamento di dati relativi all'infortunistica stradale
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia stradale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rilievo incidente

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia stradale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	Maggioli Spa

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamento violazioni stradali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia stradale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Pattugliamento stradale
Ritiro documenti
Ordinanze regolamentazione circolazione

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 28 - Polizia municipale - Trattamento di dati relativi all'attivita' di rilascio di permessi per invalidi
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia stradale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rilascio contrassegno invalidi

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia stradale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sorveglianza degli attraversamenti pedonali davanti alle scuole elementari
Sequestro di veicoli coinvolti nel sinistro

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia stradale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rimborso somme versate erroneamente per violazioni amministrative

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Polizia stradale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Acquisizione/Messa in funzione apparecchiature per controllo dei veicoli non assicurati, non revisionati, rubati

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'
AREA	SEGRETARIO GENERALE
SETTORE	SEGRETARIO GENERALE
SERVIZIO: denominazione e punti di contatto	Prevenzione della corruzione e illegalita'
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Monitoraggio funzionamento PTPCT e monitoraggio singole misure
Attivazione del sistema di tutela del dipendente che segnala illeciti
Attivita' relativa alla gestione delle segnalazioni di illeciti

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Protezione Civile
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	RISORSE E AMBIENTE SRL

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Esercitazione e formazione del personale interno
Partecipazione a coordinamenti intercomunali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Protezione Civile
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	RISORSE E AMBIENTE SRL
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Censimento dei danni e individuazione degli interventi necessari per il superamento dell'emergenza
Interventi di somma urgenza

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 40 - Ufficio Segreteria - Trattamento di dati relativi alla tenuta albi comunali Associazioni e Organizzazioni di Volontariato nonche' all'attivita' di relativa agli organismi di decentramento e di partecipazione
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Protezione Civile
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	RISORSE E AMBIENTE SRL
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA

	OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Aggiornamento dell'Elenco delle Associazioni incluse nelle attivita' di protezione civile

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Protezione Civile
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	RISORSE E AMBIENTE SRL
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Convenzioni con associazioni di volontariato

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 51 bis - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato (Obbligo DPIA)
AREA	AREA SERVIZI GENERALI
SETTORE	CULTURA, TURISMO E PROMOZIONE DELLA CITTA'
SERVIZIO: denominazione e punti di contatto	Protocollo e Archivio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il

	riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Consultazione documenti Archivio Storico Comunale

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato
AREA	AREA SERVIZI GENERALI
SETTORE	CULTURA, TURISMO E PROMOZIONE DELLA CITTA'
SERVIZIO: denominazione e punti di contatto	Protocollo e Archivio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il

	riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Consultazione documenti Archivio Storico Comunale

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione
AREA	AREA SERVIZI GENERALI
SETTORE	CULTURA, TURISMO E PROMOZIONE DELLA CITTA'
SERVIZIO: denominazione e punti di contatto	Protocollo e Archivio
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Stampa giornaliera ed annuale del registro di protocollo informatico
Annullamenti di protocollo per errata assegnazione
Archiviazione atti in archivio di deposito
Aggiornamento manuale di gestione
Scarti di archivio
Consultazione documenti Archivio Storico Comunale
Smistamento agli uffici della documentazione protocollata

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
AREA	SEGRETARIO GENERALE
SETTORE	SEGRETARIO GENERALE
SERVIZIO: denominazione e punti di contatto	SEGRETARIO GENERALE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	H.S.E. Consulting s.r.l.

trattamento: denominazione e punti di contatto	Rossi Valerio
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Medico competente
Vigilanza sanitaria a cura del medico competente
Registro dei responsabili del trattamento relativo alle attivita' di trattamento dei dati personali
Registro del titolare del trattamento dei dati personali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali
AREA	SEGRETARIO GENERALE
SETTORE	SEGRETARIO GENERALE
SERVIZIO: denominazione e punti di contatto	SEGRETARIO GENERALE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo strategico ai sensi dell'art. 147-ter del D.Lgs. 267/2000

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	SEGRETARIO GENERALE
SETTORE	SEGRETARIO GENERALE
SERVIZIO: denominazione e punti di contatto	SEGRETARIO GENERALE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo successivo di regolarita' amministrativa e contabile ai sensi dell'art. 147-bis del D.Lgs. 267/2000

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'
AREA	SEGRETARIO GENERALE
SETTORE	SEGRETARIO GENERALE
SERVIZIO: denominazione e punti di contatto	SEGRETARIO GENERALE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Giornate della Trasparenza
Gestione del rischio violazione sicurezza del trattamento dei dati personali - DPIA

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 65 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi alla verifica della legittimita', del buon andamento e dell'imparzialita' dell'attivita' amministrativa
AREA	SEGRETARIO GENERALE
SETTORE	SEGRETARIO GENERALE
SERVIZIO: denominazione e punti di contatto	SEGRETARIO GENERALE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato	

trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco

	ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento

	- MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti

	inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Consulenza e assistenza del Segretario/Direttore agli organi di indirizzo politico

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SERVIZIO APPALTI E CONTRATTI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Affidamento servizi postali
Affidamento appalto di lavori di importo pari o superiore a 40.000 euro e inferiore a 150.000 euro mediante il sistema della procedura negoziata
Affidamento appalto di lavori di importo pari o superiore a 150.000 euro e inferiore a 1.000.000 di euro mediante il sistema della procedura negoziata
Affidamento appalto di lavori di importo pari o superiore a 1.000.000 di euro mediante il sistema della procedura aperta

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SERVIZIO APPALTI E CONTRATTI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rogito atti segretario comunale
Autenticazione scritture private
Liquidazione diritti di segreteria
Registrazione
Adempimenti conseguenti alla stipula del contratto: registrazione anni successivi
Pagamento delle spese di registrazione
Vidimazione repertorio

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione
AREA	SEGRETARIO GENERALE
SETTORE	SEGRETARIO GENERALE
SERVIZIO: denominazione e punti di contatto	SERVIZIO AVVOCATURA
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione del contenzioso: Udienze GdP
Gestione del contenzioso in proprio: elaborazione controdeduzioni per GdP
Affidamento del contenzioso GdP e Tribunale alla difesa esterna mediante il sistema dell'affidamento diretto
Controversie e contenziosi esterni ed interni, citazioni, costituzioni in giudizio, e conseguente nomina dei difensori e consulenti

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 34 - Trattamento di dati relativi all'attivita' del difensore civico comunale
AREA	SEGRETARIO GENERALE
SETTORE	SEGRETARIO GENERALE
SERVIZIO: denominazione e punti di contatto	SERVIZIO AVVOCATURA
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Attivita' del difensore civico comunale - Supporto al difensore civico

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SERVIZIO CENTRALINO, MESSI E PORTINERIA
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Albo e notifiche: Notifiche

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SERVIZIO CONTROLLO DI GESTIONE
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Attivita' di valutazione della performance e assegnazione punteggi e premi - OIV/Nuclei
Nomina componenti del Nucleo di valutazione - OIV

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario
AREA	AREA SERVIZI GENERALI
SETTORE	SERVIZI FINANZIARI, TRIBUTI E DEMANIO
SERVIZIO: denominazione e punti di contatto	SERVIZIO DEMANIO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assegnazione di aree per l'edilizia residenziale pubblica

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	AREA SERVIZI GENERALI
SETTORE	SERVIZI FINANZIARI, TRIBUTI E DEMANIO
SERVIZIO: denominazione e punti di contatto	SERVIZIO DEMANIO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Aster srl - Agenzia Servizi al Territorio
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale

	Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure

	minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione)

accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA INCIDENTI: crimeware (malware che mirano a ottenere il controllo dei sistemi) - CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento -TRATTAMENTI ELETTRONICI: utilizzo di parole chiave non adeguate - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi

	punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze

	della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi - Tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di

	violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o

	tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Affidamento servizi di pulizia uffici comunali
Concessione a titolo gratuito delle sale e immobili del patrimonio comunale
Concessioni canali demaniali irrigui
Locazione immobili urbani
Vendita beni patrimonio disponibile mediante asta pubblica

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)
AREA	AREA SERVIZI GENERALI
SETTORE	SERVIZI FINANZIARI, TRIBUTI E DEMANIO
SERVIZIO: denominazione e punti di contatto	SERVIZIO DEMANIO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	SOCIETA' ELLENIA S.N.C. DI BORSATTI CLARA E C. Aster srl - Agenzia Servizi al Territorio
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Trascrizione decreti esproprio e altri

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
AREA	AREA SERVIZI GENERALI
SETTORE	SERVIZI FINANZIARI, TRIBUTI E DEMANIO
SERVIZIO: denominazione e punti di contatto	SERVIZIO FINANZIARIO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione squadre operative

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	AREA SERVIZI GENERALI
SETTORE	SERVIZI FINANZIARI, TRIBUTI E DEMANIO
SERVIZIO: denominazione e punti di contatto	SERVIZIO FINANZIARIO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamenti di entrata

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	AREA SERVIZI GENERALI
SETTORE	SERVIZI FINANZIARI, TRIBUTI E DEMANIO
SERVIZIO: denominazione e punti di contatto	SERVIZIO FINANZIARIO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Fornitura cancelleria ed altro materiale di consumo per gli uffici

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	Servizio Risorse Umane e Organizzazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	Maggioli Spa

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Certificazione in materia di spesa di personale
Liquidazione periodiche trattamenti accessori
Pensioni: Liquidazioni INPS - riscatti - ricongiunzioni
Pensioni: Pratiche
Rilascio certificato di stipendio
Stipendi-Paghe
Certificazione crediti
Rimborso oneri per datore di lavoro
Programma triennale ed annuale del fabbisogno di personale
Assunzione di personale mediante concorsi, mobilita' e contratti di lavoro a tempo determinato o flessibile
Selezioni da centro per l'impiego
Stabilizzazioni
Mobilita' dall'esterno ex art. 30 del D. Lgs. 165/2001
Mobilita' ex art. 34 bis, D. L.gs. 165/2001
Mobilita' interna intersettoriale da P.E.G.
Cambi di profilo professionale
Trasformazione del rapporto di lavoro a tempo parziale
Denunce infortuni sul lavoro
Gestione coperture INAIL
Procedimento disciplinare
Comandi e trasferimenti
Autorizzazioni a prestazioni professionali di personale interno a tempo indeterminato e determinato
Nomina componenti del CUG in quota Comune

Rilevazione eccedenze personale
Assunzioni interinali
Certificazioni e attestazioni posizioni assicurative (pa) per uso ricongiunzioni, riscatti ed altro
Certificazioni stipendio per cessione quinto
Attribuzione progressioni economiche orizzontali o di carriera
Ordinativi di incasso

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	Servizio Risorse Umane e Organizzazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assunzione disabili
Riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa
Denunce infortuni sul lavoro

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	Servizio Risorse Umane e Organizzazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	Maggioli Spa
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Liquidazione indennita' mensili amministratori

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	Servizio Risorse Umane e Organizzazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo della qualita' dei servizi

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	Servizio Risorse Umane e Organizzazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	TELECOM ITALIA SPA ARUBA PEC SPA ECOH MEDIA SRL TEAMSYSTEM SPA ABACO SPA POSTE ITALIANE SPA Day Ristoservice S.p.A. TELECOM ITALIA TRUST TECHNOLOGIES S.R.L. GLOBO Aster srl - Agenzia Servizi al Territorio Maggioli Spa
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la

	sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON

	AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche

	amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi

	del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di

	violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare

	regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Liquidazione trattamento fine mandato
Versamenti contributivi datori di lavoro

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	Servizio Risorse Umane e Organizzazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	TEAMSYSTEM SPA POSTE ITALIANE SPA ECOH MEDIA SRL ABACO SPA GLOBO TELECOM ITALIA TRUST TECHNOLOGIES S.R.L. TELECOM ITALIA SPA ARUBA PEC SPA
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON

	AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

	VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1):

	INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA INCIDENTI: crimeware (malware che mirano a ottenere il controllo dei sistemi) - CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento -TRATTAMENTI ELETTRONICI: utilizzo di parole chiave non adeguate - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle

	utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno

	semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi - Tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei

	processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione sito web: Affidamento gestione in hosting
AGID: Acquisto e consegna firme digitali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	Servizio Risorse Umane e Organizzazione
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	Aster srl - Agenzia Servizi al Territorio

trattamento: denominazione e punti di contatto	Maggioli Spa
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sicurezza dei processi - servizi informatici
Sviluppo software: Installazione/configurazione nuovo software applicativo
Sviluppo software: Acquisizione servizio di manutenzione
Gestione S.I. e rete: Acquisizione fornitura connettivita'
Gestione S.I. e rete: Configurazione connettivita'
Gestione S.I. e rete: Backup dei dati
Gestione S.I. e rete: Aggiornamento backup
Gestione S.I. e rete: Configurazione utenti di rete
Gestione S.I. e rete: Configurazione apparati di rete
Gestione S.I. e rete: Creazione caselle di posta elettronica
Gestione S.I. e rete: Aggiornamenti automatici sw di base e produttivita'
Gestione S.I. e rete: Aggiornamento antivirus
Gestione S.I. e rete: Installazione stampanti di rete
Gestione S.I. e rete: Gestione server di rete
Gestione S.I. e rete: Custodia e gestione delle password
Gestione S.I. e rete: Manuale sicurezza informatica
Assistenza utenti: Interventi di consulenza/addestramento
Assistenza utenti: Interventi manutenzione hardware/software
Assistenza utenti: Invio denunce all'agenzia dell'entrate via ENTRATEL
Assistenza utenti: Gestione banche dati on-line esterne

Assistenza utenti: Interventi supporto per la gestione dati applicativi
Assistenza utenti: INA SAIA
Assistenza utenti: Invio dati movimenti anagrafici alla GEOFOR
Gestione S.I. e rete: Analisi dei fabbisogni, programmazione e gestione della rete informatica
AGID: Dematerializzazione dei documenti

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali
AREA	AREA SERVIZI GENERALI
SETTORE	SERVIZI FINANZIARI, TRIBUTI E DEMANIO
SERVIZIO: denominazione e punti di contatto	SERVIZIO TRIBUTI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	ICA - Imposte Comunali e Affini SRL

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Iscrizione a ruolo entrate tributarie
Certificati relativi a posizioni tributarie
Richieste accertamento con adesione
Provvedimenti in autotutela per tributi comunali
Risposte a istanze, comunicazioni, richieste di informazioni opposizioni
Rimborsi a contribuenti-riversamenti a Comuni competenti - sgravi di quote indebite e inesigibili di tributi comunali
Istanze interpello

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	AREA SERVIZI GENERALI
SETTORE	SERVIZI FINANZIARI, TRIBUTI E DEMANIO
SERVIZIO: denominazione e punti di contatto	SERVIZIO TRIBUTI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	COMANDO PROVINCIALE DELLA GUARDIA DI FINANZA DI MANTOVA

contatto	
Responsabile trattamento: denominazione e punti di contatto	Aster srl - Agenzia Servizi al Territorio
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accertamenti tributari
Controllo ICI - IMU - TASI
Controllo Imposta di soggiorno

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche
AREA	AREA SERVIZI GENERALI
SETTORE	SERVIZI FINANZIARI, TRIBUTI E DEMANIO
SERVIZIO: denominazione e punti di contatto	SERVIZIO TRIBUTI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	ICA - Imposte Comunali e Affini SRL
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rateazione pagamento tributi accertati

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Servizi Vari
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	CONSORZIO PROGETTO SOLIDARIETA'

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gravissime disabilita'

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 13 - Servizi sociali - Trattamento di dati relativi all'attivita' ricreative per la promozione del benessere della persona e della comunita', per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Servizi Vari
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Segretariato sociale

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Servizi Vari
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	CONSORZIO PROGETTO SOLIDARIETA'

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sostegno ad associazioni operanti nell'ambito socio-educativo
Controllo I.S.E.E. per prestazioni sociali agevolate

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Servizi Vari
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	SOL.CO. TRASPORTI - Societa' Cooperativa Onlus
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Trasporto urbano

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Servizi Vari
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	ALER CONSORZIO PROGETTO SOLIDARIETA'

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assegnazione Alloggi Edilizia Residenziale Pubblica - E.R.P.
Servizio ATER

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 31 - Politiche del lavoro - Trattamento di dati relativi all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Servizi Vari
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	CONSORZIO PROGETTO SOLIDARIETA'

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per

	favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Politiche del lavoro - Gestione delle attivita' relative all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 55 - Servizi Sociali - Trattamento di dati relativi all'attivita' di gestione dell'accoglienza dei richiedenti asilo e rifugiati da parte degli enti locali partecipanti al "Sistema di protezione dei richiedenti asilo e rifugiati"
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Servizi Vari
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	CONSORZIO PROGETTO SOLIDARIETA'

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-11 - PRESCRIZIONI: nell'attivita' di videosorveglianza prescrizione del rispetto di tutte le misure e gli accorgimenti prescritti Autorita' Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs.

	196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - PROCEDURA OPERATIVA (PO): definire e attuare procedura operativa per dare attuazione, nell'attivita' di videosorveglianza, al principio di c.d. proporzionalita' nella scelta delle modalita' di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonche' nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalita' perseguite - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o

	tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio per richiedenti protezione internazionale

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SINDACO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Attribuzione incarichi dirigenziali
Nomina e revoca assessori
Nomina Segretario generale
Nomina Organismo di valutazione
Attribuzione e revoca incarichi al personale dirigente
Costituzione di ufficio posto alle dirette dipendenze del sindaco ai sensi dell'art. 90, TUEL

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina

	un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SINDACO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI

Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli	Alto

interessati	

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di

	sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti

	- MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del

	Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e

	restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Designazione e revoca dei rappresentanti del Comune presso enti, aziende e istituzioni

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SINDACO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Ordinanze in qualita' di Ufficiale di governo

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	Sportello unico per le attivita' produttive
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	ICA - Imposte Comunali e Affini SRL

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Commercio su aree pubbliche con posteggio in mercati - Controllo autorizzazioni
Concessioni per occupazione temporanee di suolo pubblico - controllo

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 29 - Trattamento di dati relativi al rilascio delle licenze e autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	Sportello unico per le attivita' produttive
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	IMPRESA IN UN GIORNO - UNIONCAMERE
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga,

	impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in

	relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il

	riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' di lavanderia
Segnalazione certificata di inizio attivita' (SCIA) per ascensori
Commercio su aree pubbliche con posteggio in mercati - Autorizzazione
Commercio itinerante su aree pubbliche - Autorizzazione
Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' di Acconciatore, Estetista, Esecuzione tatuaggi e piercing
Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' circhi
Segnalazione certificata di inizio attivita' (SCIA) per esercizi di commercio al dettaglio - media struttura di vendita con superficie fino a mq. 1.500
Segnalazione certificata di inizio attivita' (SCIA) per attivita' ricettive complementari: attivita' agrituristica-Bed and Breakfast, affittacamere
Distributori di carburanti - Autorizzazione
Esercizi di commercio al dettaglio grandi strutture di vendita - Autorizzazione
Esercizi pubblici: apertura e trasferimento di pubblico esercizio in zona non sottoposta a tutela - Autorizzazione
Trasferimento di residenza di titolare in autorizzazione per l'attivita' di commercio al dettaglio su aree pubbliche in forma itinerante e richiesta nuova - Autorizzazione
Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione di alimenti e bevande - nuova apertura
Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione di alimenti e bevande - subingresso
Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione di alimenti e bevande - trasferimento
Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione in circolo privato
Segnalazione certificata di inizio attivita' (SCIA): esercizio di somministrazione temporanea di alimenti e bevande in occasione di manifestazioni

Noleggio di veicoli con conducente - Autorizzazione
Noleggio di veicoli senza conducente - Autorizzazione
Pubblica sicurezza: falo' tradizionale - Autorizzazione
Pubblica sicurezza: fuochi d'artificio - Autorizzazione
Pubblica sicurezza: Lotteria, tombola e pesca di beneficenza - Autorizzazione
Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' ricettive complementari: case vacanze
Pubblica sicurezza: mestiere di fochino - Autorizzazione
Pubblica sicurezza: palestre - Autorizzazione
Pubblica sicurezza: rimessa veicoli - Autorizzazione
Pubblica sicurezza: strumenti da punta e da taglio - Autorizzazione
Rivendite di quotidiani e periodici - Autorizzazione
Commercio itinerante su aree pubbliche e su posteggio - subingresso - Autorizzazione
Taxi - Autorizzazione
Segnalazione certificata di inizio attivita' (SCIA): commercio elettronico, vendita per corrispondenza, televisione
Segnalazione certificata di inizio attivita' (SCIA): vendita al dettaglio a domicilio
Manifestazioni fieristiche-Fiere - Autorizzazione
Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' di giochi leciti e videogiochi
Pubblica sicurezza: istruttore / direttore di tiro a segno - Autorizzazione
Segnalazione certificata di inizio attivita' (SCIA): vendita diretta da parte dei produttori agricoli
Attivita' funebre - Autorizzazione
Segnalazione certificata di inizio attivita' (SCIA) per l'esercizio attivita' ricettive complementari: strutture ricettive all'aria aperta - campeggi
Segnalazione certificata di inizio attivita' (SCIA)
Segnalazione certificata di inizio attivita' (SCIA): commercio all'ingrosso nel settore alimentare
Segnalazione certificata di inizio attivita' (SCIA): stabilimenti industriali
Vendita ambulante di strumenti da punta e da taglio - Autorizzazione
Segnalazione certificata di inizio attivita' (SCIA): commercio di prodotti agricoli e zootecnici, mangimi, prodotti di origine minerale e chimico industriali destinati all'alimentazione animale
Segnalazione certificata di inizio attivita' (SCIA): somministrazione di alimenti e bevande tramite mense, ristorazione collettiva nell'ambito di case di riposo, ospedali, scuole, caserme, comunita' religiose
Segnalazione certificata di inizio attivita' (SCIA): somministrazione di alimenti e bevande nell'ambito di altre attivita' quali sale giochi, sale scommesse autorizzate ai sensi del TULPS (Testo unico leggi di pubblica sicurezza)
Segnalazione certificata di inizio attivita' (SCIA) attivita' artigianali in genere, compresi i laboratori di produzione, di trasformazione e/o confezionamento con/senza attivita' di vendita diretta al consumatore finale
Segnalazione certificata di inizio attivita' (SCIA): somministrazione di alimenti e bevande nell'ambito di musei, teatri, sale da concerti
Segnalazione certificata di inizio attivita' (SCIA): somministrazione di alimenti e bevande nell'ambito di altre attivita' quali sale da ballo, locali notturni, stabilimenti balneari, impianti sportivi
Segnalazione certificata di inizio attivita' (SCIA): variazione della superficie degli esercizi pubblici di somministrazione alimenti e bevande

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	SPORTELLO UNICO IMPRESE E CITTADINI
SERVIZIO: denominazione e punti di contatto	Sportello unico per le attivita' produttive
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo COSAP

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Sport e tempo libero
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di	

contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione

	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non

	adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione)

indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni'

	e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale

	- MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento

	consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e

	attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Richiesta di premi in occasione di manifestazioni sportive
Contributi straordinari a concessionari di impianti
Contributi per manifestazioni
Contributi ad associazioni sportive dilettantistiche

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Sport e tempo libero
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Promozione attivita' di educazione sportiva scuole
Autorizzazione per eventi e manifestazioni negli impianti sportivi comunali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	Area Servizi ai cittadini
SETTORE	WELFARE SERVIZI SOCIALI E SPORT
SERVIZIO: denominazione e punti di contatto	Sport e tempo libero
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessione in gestione impianti sportivi

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SUPPORTO ORGANI ISTITUZIONALI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assistenza organi istituzionali: Gestione sedute commissioni consiliari
Assistenza organi istituzionali: Gestione sedute conferenze capigruppo
Assistenza organi istituzionali: Gestione sedute Consiglio comunale
Assistenza organi istituzionali: Trascrizione verbali consiglio
Assistenza organi istituzionali: Surroghe
Assistenza organi istituzionali: Convalida consiglieri
Assistenza organi istituzionali: Approvazione verbali consiglio
Assistenza organi istituzionali: Nomina Presidente e vicepresidenti
Assistenza organi istituzionali: Decadenze
Assistenza organi istituzionali: Fornitura servizi ai gruppi consiliari
Assistenza organi istituzionali: Determinazione indennita' amministratori
Assistenza organi istituzionali: Gestione sedute Giunta comunale
Anagrafe degli eletti: Pubblicazione e aggiornamento dati on line

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SUPPORTO ORGANI ISTITUZIONALI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Redazione delibera/determina

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SUPPORTO ORGANI ISTITUZIONALI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Albo e inviti: Inviti consigli comunali
Albo e notifiche: Pubblicazioni albo on line

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	SUPPORTO ORGANI ISTITUZIONALI
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Archiviazione deliberazioni/determinazioni

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
AREA	TUTTE LE AREE - ATTIVITA' TRASVERSALE
SETTORE	Tutti i settori - Attivita' trasversale
SERVIZIO: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Partecipazione a corsi di formazione
Nomina Responsabile Unico del Procedimento (RUP)
Conferimento di incarichi di collaborazione, studio e ricerca nonche' di consulenza a soggetti estranei all'amministrazione

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 35 - Trattamento di dati relativi agli istituti di democrazia diretta
AREA	TUTTE LE AREE - ATTIVITA' TRASVERSALE
SETTORE	Tutti i settori - Attivita' trasversale
SERVIZIO: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Attivita' riguardante gli istituti di democrazia diretta

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche
AREA	TUTTE LE AREE - ATTIVITA' TRASVERSALE
SETTORE	Tutti i settori - Attivita' trasversale
SERVIZIO: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Liquidazione fatture

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA
(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate

	dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'
AREA	TUTTE LE AREE - ATTIVITA' TRASVERSALE
SETTORE	Tutti i settori - Attivita' trasversale
SERVIZIO: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Aster srl - Agenzia Servizi al Territorio
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita'

	naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure

	minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e

	software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di

	sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre

	- MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari

	- MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati

	- MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Pubblicazioni su Amministrazione trasparente di dati, informazioni e documenti
Segnalazione-Esposto
Segnalazioni dipendenti

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento
AREA	TUTTE LE AREE - ATTIVITA' TRASVERSALE
SETTORE	Tutti i settori - Attivita' trasversale
SERVIZIO: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il

	riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Convenzioni, transazioni ed ogni disposizione patrimoniale di straordinaria amministrazione
Accordi integrativi o sostitutivi del provvedimento
Autorizzazione al ricorso a transazioni e altri rimedi di risoluzione delle controversie alternativi a quelli giurisdizionali

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	TUTTE LE AREE - ATTIVITA' TRASVERSALE
SETTORE	Tutti i settori - Attivita' trasversale
SERVIZIO: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Acquisto arredi e attrezzature uffici
Fornitura vestiario e calzature personale
Proroga contratto in scadenza
Adesione convenzioni CONSIP o del Soggetto Aggregatore di riferimento
Affidamento appalto di lavori, servizi e forniture di importo inferiore a 40.000 euro tramite il sistema dell'affidamento diretto
Affidamento appalto di servizi e forniture di importo superiore alle soglie di cui all'art. 35, D. Lgs. 50/2016 attraverso il sistema della procedura aperta
Affidamento appalto di servizi e forniture di importo pari o superiore a 40.000 euro e inferiore alle soglie di cui all'articolo 35, D. Lgs. 50/2016 mediante il sistema della procedura negoziata

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato
AREA	TUTTE LE AREE - ATTIVITA' TRASVERSALE
SETTORE	Tutti i settori - Attivita' trasversale
SERVIZIO: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il

	riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accesso art. 43, co. 2 del T.U.E.L. da parte dei consiglieri
Accesso civico semplice concernente dati, documenti e informazioni soggetti a pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013
Accesso art. 22 e segg. della L. 241/90
Accesso art. 43, co. 2 del T.U.E.L. da parte dei consiglieri
Accesso civico generalizzato concernente dati e documenti ulteriori a quelli soggetti a pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013
Registro degli accessi

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente
AREA	TUTTE LE AREE - ATTIVITA' TRASVERSALE
SETTORE	Tutti i settori - Attivita' trasversale
SERVIZIO: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Formazione Albo dei professionisti esterni

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione
AREA	TUTTE LE AREE - ATTIVITA' TRASVERSALE
SETTORE	Tutti i settori - Attivita' trasversale
SERVIZIO: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	Aster srl - Agenzia Servizi al Territorio

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione e acquisizione degli atti e della posta in arrivo e in partenza per la registrazione sul protocollo informatico
Accettazione, protocollazione e smistamento delle partecipazioni a gare
Smistamento agli uffici della documentazione protocollata
Tenuta archivio corrente
Accettazione, protocollazione e smistamento delle partecipazioni a gare
Smistamento agli uffici della documentazione protocollata

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 19 - Servizi sociali - Trattamento di dati relativi ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Ufficio amministrativo
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Molto alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Trattamenti sanitari obbligatori (T.S.O.) ed assistenza sanitaria obbligatoria (A.S.O.)

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Ufficio amministrativo
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Ordinanze di confisca e provvedimenti di dissequestro
Annullamento d'ufficio di verbali per violazioni a norme di legge nazionale o regionale
Ordinanza di ingiunzione

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Ufficio amministrativo
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare

	tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sequestri denaro o cose ai sensi del Reg. di P.U.

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Ufficio amministrativo
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati

	personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sospensione attivita'
Provvedimento per l'esecuzione d'ufficio in caso di mancata ottemperanza da parte dei destinatari a quanto precedentemente ordinato

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi
AREA	POLIZIA LOCALE
SETTORE	Settore polizia locale
SERVIZIO: denominazione e punti di contatto	Ufficio amministrativo
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento:	

denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)

	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della

modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva degli interessati	violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle

	'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali

	assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento,

	in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

	- MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Convenzione per adesione al servizio di consultazione Archivio Veicoli Rubati C.E.D. Interforze tramite i servizi telematici Ancitel

Convenzione per adesione all'utenza per il servizio di consultazione del C.E.D. della Direzione Generale della Motorizzazione Civile - Ministero delle Infrastrutture

Convenzione per la fornitura, mediante supporto informatico, di dati contenuti nel sistema informativo del Pubblico registro Automobilistico

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE
DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni
AREA	AREA SERVIZI GENERALI
SETTORE	AFFARI GENERALI E ISTITUZIONALI
SERVIZIO: denominazione e punti di contatto	UNITA' ORGANIZZATIVA GABINETTO DEL SINDACO
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	

Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet

	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO

	APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati,	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare)

rilevati dalla prospettiva degli interessati	- Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative

	implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il

	periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli

	incaricati medesimi; c) al controllo, alla custodia e restituzione della documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza

	prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Agenda Sindaco ed Assessori
Rapporti con Presidente CC

Comune di MANTOVA
Via Roma 39
46100 MANTOVA Mantova

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE

SINTESI DPIA

DA PUBBLICARE SU SITO WEB DEL TITOLARE/RESPONSABILE DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA

(da esibire su richiesta dell'Autorita' di controllo)

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	12/12/2019
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete
AREA	AREA POLITICHE DEL TERRITORIO
SETTORE	TERRITORIO E LAVORI PUBBLICI
SERVIZIO: denominazione e punti di contatto	Urbanistica
Titolare trattamento: denominazione e punti di contatto	Comune di MANTOVA Palazzi Mattia
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile	

trattamento: denominazione e punti di contatto	
Sub-Responsabile/Incaricato trattamento: denominazione e punti di contatto	

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI	
Origine dei rischi rilevati dalla prospettiva degli interessati	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati

	tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco

	ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni)
Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati, rilevati dalla prospettiva	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

degli interessati	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati rilevati dalla prospettiva degli interessati	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni "point-of-sale" - CAUSA DI INCIDENTI: web app tracks
Stima della probabilita' e gravita' rilevata dalla prospettiva degli interessati	Alto

MISURE PREVISTE PER AFFRONTARE I RISCHI	
Misure tecniche informatiche	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)

	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato ,incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza - MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative - MS-ICT-13 - Realizzazione di ambienti di ricovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-14 - Una vulnerability assessment periodica, e almeno semestrale o annuale, sulla architettura informatica effettuata da soggetti specializzati e diversi dai Responsabili dei servizi informativi del titolare, condotta specie con riferimento alle vulnerabilita' dei software che potrebbero essere sfruttate dagli attaccanti per compiere le intrusioni informatiche e con formale approvazione delle risultanze della vulnerability assessment da parte dell'organo di governo dell'ente
Misure tecniche logistiche	- MS-LOG-04 - PROTEZIONE AREE E LOCALI: nomina, per ciascun ufficio, dell'incaricato della custodia delle aree e dei locali assegnando allo stesso i compiti relativi con atto formale - MS-LOG-07 - PROTEZIONE AREE E LOCALI: definizione, per il periodo al di fuori dell'orario di lavoro, di modalita' di accesso dei

	dipendenti agli uffici in cui sono presenti sistemi o apparecchiature di accesso di dati trattati - MS-LOG-02 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/Impianto antincendio e, ove possibile: sensori, allarmi, porte taglia fuoco, porte antincendio per fuga, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti - MS-LOG-05 - PROTEZIONE AREE E LOCALI: identificazione incaricati autorizzati ad accedere ai locali e a ricevere la consegna delle chiavi - MS-LOG-03 - PROTEZIONE AREE E LOCALI: sorveglianza dei locali in caso di temporanee assenze dei dipendenti - MS-LOG-01 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: sistema di allarme interno e/o esterno, e serrature in tutte le porte degli uffici, sensori, connessione con le forze dell'ordine, connessione con servizi di vigilanza, videosorveglianza, porta blindata, grate e inferiate alle finestre - MS-LOG-06 - PROTEZIONE AREE E LOCALI: dettagliate istruzioni agli incaricati per la chiusura degli uffici durante la loro assenza, anche temporanea - MS-LOG-08 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere - MS-LOG-09 - PROTEZIONE AREE E LOCALI: norme comportamentali nelle lettere di delega/incarico sulla custodia delle aree, dei locali e delle chiavi
Misure organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-02 - WORK FLOW: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento - MS-ORG-01 - WORK FLOW: In applicazione dei principi della norma UNI ISO 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-ORG-12 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici, con riferimento, in particolare: a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) alle istruzioni da impartire agli incaricati medesimi; c) al controllo, alla custodia e restituzione della

	documentazione; d) al controllo degli accessi degli archivi/banche dati - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti
Misure procedurali	- In applicazione dei principi della norma UNI ISO 31000, integrare la gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti - MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-04 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali - MS-PO-03 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-06 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel

	provvedimento del Garante n. 393 del 2 luglio 2015 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, e non espressamente indicate - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-08 - DISCIPLINARE TECNICO-PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003, che il titolare intende attuare benche' abrogato, per i trattamenti con strumenti diversi da quelli elettronici: a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi; c) le modalita' del controllo, custodia e restituzione della documentazione; d) le modalita' del controllo degli accessi agli archivi/banche dati - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

ELENCO TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione tecnologica SIT: Affidamento censimento edifici, foto, numerazione interna
Gestione tecnologica SIT: Creazione banca dati geografica
Gestione tecnologica SIT: Interventi per la normalizzazione delle banche dati comunali
Gestione tecnologica SIT: Formazione GIS