COMUNITA' MONTANA VALLE TROMPIA
Via G. Matteotti, 327
25063 Gardone Val Trompia

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)

ALLEGATO N. 10

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	22/05/2018
Stato del documento	In fase di analisi
Estensori del documento	- Titolare del trattamento con l'assistenza del RTD e con la consulenza del RPD, di eventuali esperti di settore, del responsabile della sicurezza dei sistemi informativi e del responsabile IT
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	- Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA

TIPOLOGIA TRATTAMENTO	
Denominazione del trattamento	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita' (Obbligo di DPIA)
Area	TUTTE LE AREE - ATTIVITA' TRASVERSALE
Settore	TUTTI E SETTORI - Attivita" trasversale
Ufficio: denominazione e punti di contatto	Tutti gli uffici - Attivita' trasversale
Titolare trattamento: denominazione e punti di contatto	Comune di COMUNITA MONTANA VALLE TROMPIA Ottelli Massimo
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 chiavi con violazione misure minime ABSC 5 (CSC 5): 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	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, 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 1) - 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-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 -MS-LOG-10- PROTEZIONE AREE E LOCALI: serrature in tutte le porte degli uffici, servizio di sorveglianza notturna, porta blindata, grate e inferiate alle finestre, chiusura automatica porta esterna
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 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 interessatiin 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 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-Esposto
Segnalazioni dipendenti
Gestione del rischio violazione sicurezza del trattamento dei dati personali - DPIA