**PIANO DI PROTEZIONE DEI DATI PERSONALI**

**E GESTIONE DEL RISCHIO DI VIOLAZIONE**

**DPIA- FASE 2**

**VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[[1]](#footnote-1)**

Documento per provare ed essere in grado di dimostrare che

il trattamento e' effettuato conformemente al RGPD

**ALLEGATO N. XX**

|  |  |
| --- | --- |
| **SETTORE** | 03 SETTORE SERVIZI SOCIO-ASSISTENZIALI |
| **SERVIZIO** | Affari sociali |
| **UFFICIO** | Affari Sociali |

|  |  |
| --- | --- |
| **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.) |

|  |  |
| --- | --- |
| **Abbinamento del trattamento ad un insieme di trattamenti simili** | La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*.  Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**.  L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento. |

|  |  |
| --- | --- |
| **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** | 22/07/2019 |
| **Stato del documento** | Approvato |
| **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** | - Pubblicazione DPIA o di una sintesi della DPIA sul sito web dell'Ente, in caso di svolgimento della DPIA |

**RISCHIO ELEVATO E OBBLIGO DI DPIA**

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").

La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata 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 ( di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.

La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

**OBIETTIVI DA RAGGIUNGERE**

La DPIA e' funzionale alla gestione del rischio[[2]](#footnote-2), per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.

L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.

In questo quadro, la DPIA intende fungere da strumento:

* che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
* che consente di comprovare la conformita' del sistema al RGPD.

**DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI**

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

* assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA
* raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate
* documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
* se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)
* sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

* assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;

d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

**CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA**

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

|  |  |
| --- | --- |
| a) | una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; |

|  |  |
| --- | --- |
| b) | una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita'; |

|  |  |
| --- | --- |
| c) | una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e |

|  |  |
| --- | --- |
| d) | le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. |

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

**SEZIONE I**

**DESCRIZIONE SISTEMATICA**

**DEL TRATTAMENTO PREVISTO E DELLE FINALITA'**

**compreso, ove applicabile, l'interesse legittimo perseguito dal titolare**

**(art. 35, paragrafo 7, lettera a)**

|  |  |
| --- | --- |
| **SETTORE** | 03 SETTORE SERVIZI SOCIO-ASSISTENZIALI |
| **SERVIZIO** | Affari sociali |
| **UFFICIO:** denominazione e punti di contatto | Affari Sociali |
| **Titolare trattamento:** denominazione e punti di contatto | Comune di PORTO CESAREO  SINDACO Albano Salvatore |
| **Contitolare/i trattamento:** denominazione e punti di contatto | Ambito Territoriale |
| **Responsabile trattamento:** denominazione e punti di contatto | Il Sorriso s.n.c.  Ambaraba' Coop Sociale  Comunita' Emmanuel Lecce |
| **Sub-Responsabile:** denominazione e punti di contatto |  |
| **Delegato trattamento:** denominazione e punti di contatto | Giaccari Maria Antonietta |
| **Incaricati trattamento:** denominazione e punti di contatto | Rizzello Maurizio |

|  |
| --- |
| **Sintetica descrizione del trattamento e del flusso informativo** |

Scheda n. 19 - I dati vengono acquisiti sia mediante la certificazione medica trasmessa dal servizio di igiene mentale sia tramite comunicazioni di soggetti terzi (Polizia municipale, Forze di polizia); in seguito alla redazione dell'ordinanza, viene individuato il luogo di ricovero del paziente ed inviata l'opportuna comunicazione al giudice tutelare per la convalida del provvedimento, di cui ne viene altresi' data comunicazione al sindaco della citta' di residenza dell'interessato, che procede ad eseguire le annotazioni di legge nel registro anagrafico ovvero al Ministero dell'interno, e al consolato competente, tramite il prefetto nel caso di cittadini stranieri o di apolidi.

|  |  |  |
| --- | --- | --- |
| **RGPD** | | **FRAMEWORKS FUNZIONE** |
| art.35 lett.a) | | Descrivere |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** | |
| **Fonte normativa** | - Scheda n. 19 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo  L. 13.05.1978, n. 180 - L. 23.12.1978, n. 833 | |
| **Natura del trattamento** | - Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati | |
| **Ambito di applicazione del trattamento** | - Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016  - Trattamento in ambito pubblico  - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici | |
| **Nome archivio/Banca dati** | - Scheda n. 19 - Sistema informativo relativo a trattamenti Sanitari Obbligatori - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014 | |
| **Tipo di archivio/Banca dati** | - i dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei | |
| **Categorie-tipi di dati** | - Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003)  - Dati idonei a rilevare lo stato di salute: patologie attuali  - Dati idonei a rilevare lo stato di salute: patologie pregresse  - Dati idonei a rilevare lo stato di salute: terapie in corso  - Dati idonei a rilevare lo stato di salute: anamnesi familiare | |
| **Luoghi di custodia dei dati** | - In Italia  - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi | |
| **Finalita' del trattamento** | - Scheda n. 19 - Trattamento effettuato per finalita' di assistenza sanitaria. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare | |
| **Rilevanti finalita' di interesse pubblico** | - Scheda n. 19 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonche' compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumita' fisica ai sensi dell'art. 2-sexies, comma 2, lett. u), D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (interventi di rilievo sanitario) | |
| **Interesse legittimo perseguito** | - Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore) | |
| **Categorie di trattamenti- forme ordinarie di elaborazione** | - Trattamento 'ordinario' dei dati-operazioni eseguite: a) raccolta presso gli interessati  - Trattamento 'ordinario' dei dati-operazioni eseguite: a) elaborazione in forma cartacea  - Trattamento 'ordinario' dei dati-operazioni eseguite: b) elaborazione con modalita' informatizzate  - Trattamento 'ordinario' dei dati-operazioni eseguite: b) raccolta di dati presso terzi | |
| **Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*** | - Scheda n. 19 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa):  a) sindaco della citta' di residenza (per effettuare le annotazioni di legge);  b) giudice tutelare ed, eventualmente, sindaco del comune di residenza, nonche' al Ministero dell'interno, e al consolato competente, tramite il prefetto nel caso di cittadini stranieri o di apolidi (per la convalida del provvedimento);  c) luoghi di ricovero (per l'effettuazione della prestazione)  - Altre amministrazioni ed enti pubblici  - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ai soggetti interconnessi | |
| **Categorie di trattamenti - particolari forme di elaborazione: *diffusione*** | N.R. | |
| **Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*** | - I dati personali, oggetto di trattamento, non vengono trasferimenti a un paese terzo o a un'organizzazione internazionale | |
| **Categorie di trattamenti - particolari forme di elaborazione:** ***trattamento effettuato tramite un sito web-nome del dominio del sito web*** |  | |
| **Categorie di trattamenti - particolari forme di elaborazione:** ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*** |  | |
| **Categorie di interessati** | - Malati gravi o sottoposti a particolari trattamenti di cura | |
| **Categorie di destinatari** | - Sindaco  - Giudice tutelare  - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile o contitolare del trattamento (artt. 26 e 28 Reg.UE n. 679/2014) | |
| **Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*** | Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia | |
| **Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*** |  | |
| **Cessazione trattamento: *Periodo di conservazione dei dati*** | - I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati | |
| **Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*** | - Termine ultimo identificato dalla normativa di settore dello specifico ambito di intervento o, comunque, in base al criterio della cancellazione immediatamente dopo il "periodo minimo indispensabile di trattamento dei dati" | |
| **Cessazione trattamento: *modalita' di cessazione dei dati*** | - Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione | |
| **Parere RPO/RTD** | - E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto | |
| **Opinioni interessati o loro rappresentanti** | - E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione | |
| **Rispetto codici di condotta approvati** | - Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013 | |
| **Adesione ad un meccanismo di certificazione** | - Non risulta l'adesione a un meccanismo di certificazione | |
| **Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali** | - La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili | |

**SEZIONE II**

**VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO**

**E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD**

**(art. 35, paragrafo 7, lettera b)**

1. **NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| **art**.35 lett.b) | **Valutare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'** | - Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime  - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita'  - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati  - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati |
| **Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'** | - Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili  - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica  - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare  - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti  - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico  - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato  - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC |

**A) CONFORMITA' RGPD**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| art.35 lett.d) | **Valutare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Misure previste per dimostrare la conformita' al RGPD** | - Tracciabilita' documentale del processo decisionale di gestione del rischio |

**SEZIONE III**

**VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI**

**(art. 35, paragrafo 7, lettera c)**

**A) RISCHI**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| art.35 lett.c) | **Valutare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **RISCHI**  **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati***  (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) |
| **RISCHI**  **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 |
| **PROBABILITA' = X**  (rilevata dalla prospettiva degli interessati) | Medio |
| **GRAVITA' = Y**  (rilevata dalla prospettiva degli interessati) | Molto alto |
| **STIMA (XxY)**  **DELLA PROBABILITA' E GRAVITA'**  (rilevata dalla prospettiva degli interessati) | Molto alto |

**MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA**

* Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:
* - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;

- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

* + - *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
    - *2 = medio =* e' **improbabile** che la minaccia si possa verificare
    - *3 = alto* = *=* e' **probabile** che la minaccia si possa verificare
    - *4 = molto alto =* e' **altamente probabile** che la minaccia si possa verificare
  + **- IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  + - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).
    - *1 = basso-trascurabile*
    - *2 = medio*
    - *3 = alto*
    - *4 = molto alto*
    - La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

**Valore del rischio da 1 a 2 = RISCHIO BASSO** (verde)

**Valore del rischio da 3 a 4 = RISCHIO MEDIO** (giallo)

**Valore del rischio da 6 a 9 = RISCHIO ALTO** (arancione)

**Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO** (rosso)

* + 

La stima del rischio costituisce l'input per definire e selezionare:

* le politiche di sicurezza
* le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

**B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI**

|  |  |  |
| --- | --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** | **RISCHI CONTRASTATI** |
| art.35 lett.c) | **Proteggere** | Come da MAPPA dei rischi contrastati |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** | |
| **Misure di sicurezza:**  **tecniche logistiche** | - 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-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-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte  - MS-LOG-16 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione, ove possibile, di: serrature in tutte le porte degli uffici, porta blindata, grate e inferiate alle finestre del piano terra  - MS-LOG-17 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con dotazione di estintori/Impianto antincendio e, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti | |
| **Misure di sicurezza:**  **tecniche informatiche, comprese le misure di ripristino in caso di data breach** | - 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) | |
| **Misure di sicurezza:**  **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-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  - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi  - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi  - MS-ORG-24 - SISTEMA GESTIONE PRIVACY: piano di disaster recovery | |
| **Misure di sicurezza:**  **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. | |

**C) RISCHIO RESIDUO**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| art.36 lett.c) | **Valutare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Livello rischio dopo l'applicazione delle misure** | - Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate |

**D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| art.36 | **Consultare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
|  |  |

**SEZIONE IV**

**DOCUMENTAZIONE**

**(art. 24, paragrafo 1)**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS**  **FUNZIONE** |
| art.24 | **Documentare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Documentare la conformita' al RGPD** | - La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento . |

**SEZIONE IV**

**MONITORAGGIO E RIESAME DPIA**

**( art. 35, paragrafo 11)**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS**  **FUNZIONE** |
| art. 35 | **Monitorare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Stato attuazione misure** | - Parzialmente attuate |
| **Fasi attuazione misure** | - Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1  - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3  - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2  - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4 |
| **Indicatori attuazione misure** | - Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato  - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato |
| **Responsabile attuazione misure** | Responsabile di Settore |

|  |  |  |
| --- | --- | --- |
| **RIESAME DPIA** | | |
| **Motivazione riesame** | - La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto |

|  |
| --- |
| **ELENCO DEI TRATTAMENTI**  **INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI** |

Trattamenti sanitari obbligatori (T.S.O.) ed assistenza sanitaria obbligatoria (A.S.O.)

1. Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile" [↑](#footnote-ref-1)
2. Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative. [↑](#footnote-ref-2)