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

DPIA
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento è effettuato conformemente al GDPR

SETTORE	SETTORE STAFF DEL SINDACO
SERVIZIO	Corpo di Polizia Locale
UFFICIO	Vigilanza territoriale

TRATTAMENTO	Trattamento dei dati relativi alle attività di controllo attraverso l'installazione di sistemi di rilevazione delle immagini per fini di sicurezza pubblica.

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralità 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 finalità 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, è contenuto in calce al presente documento.

Titolo del Documento	Valutazione di impatto sulla protezione dei dati (DPIA) conforme alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità 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 è effettuato conformemente al GDPR. Ogni singola valutazione che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi
Numero di versione	001
Data ultimo aggiornamento	29-02-2024
Stato del documento	
Estensori del documento	

1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

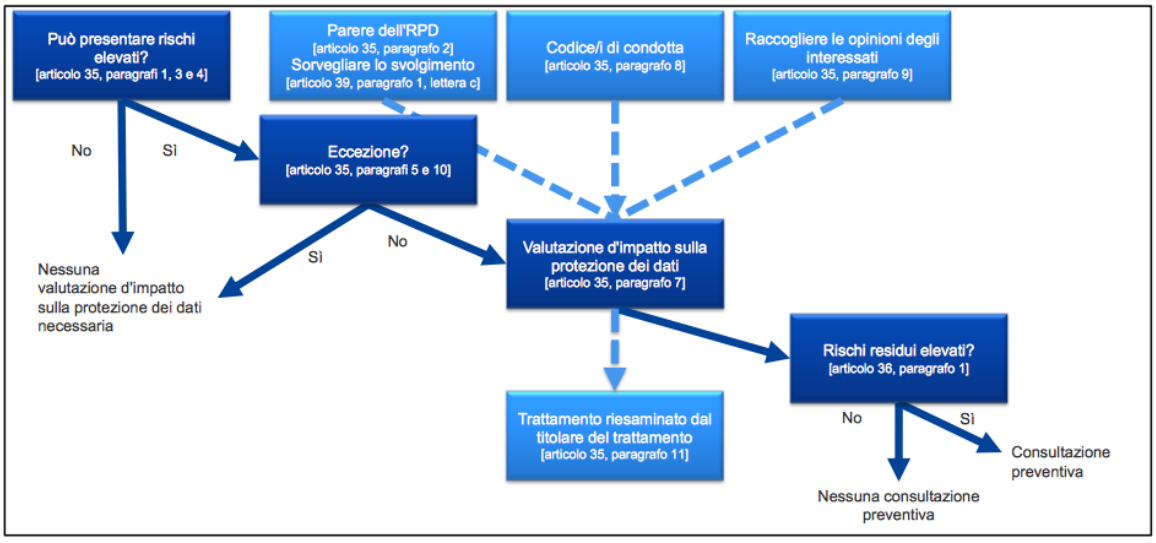
Riferimento per comunicazioni in merito al documento	Enrico Contiero
Modalità di distribuzione del presente documento e delle eventuali nuove versioni	

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilità 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 libertà delle persone fisiche, e non rientra tra le eccezioni per le quali non è 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 "GDPR").

La determinazione sulla possibilità di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilità 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 possibilità 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 **tracciabilità documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformità al GDPR in caso di richiesta dell'Autorità di controllo.

OBIETTIVI DA RAGGIUNGERE

La DPIA è funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attività coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.

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

2 Al fine di poter gestire i rischi per i diritti e le libertà delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non può per contro sottrarsi alla responsabilità coprendo i rischi stipulando polizze assicurative.

di circolazione, il divieto di discriminazione, il diritto alla libertà 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 conformità del sistema al GDPR.

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, così 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, altresì, la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che ciò 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 tracciabilità 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 qualità della valutazione dei rischi e del grado di accettabilità del rischio residuo, nonché 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, nonché 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) nonché 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 GDPR:

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

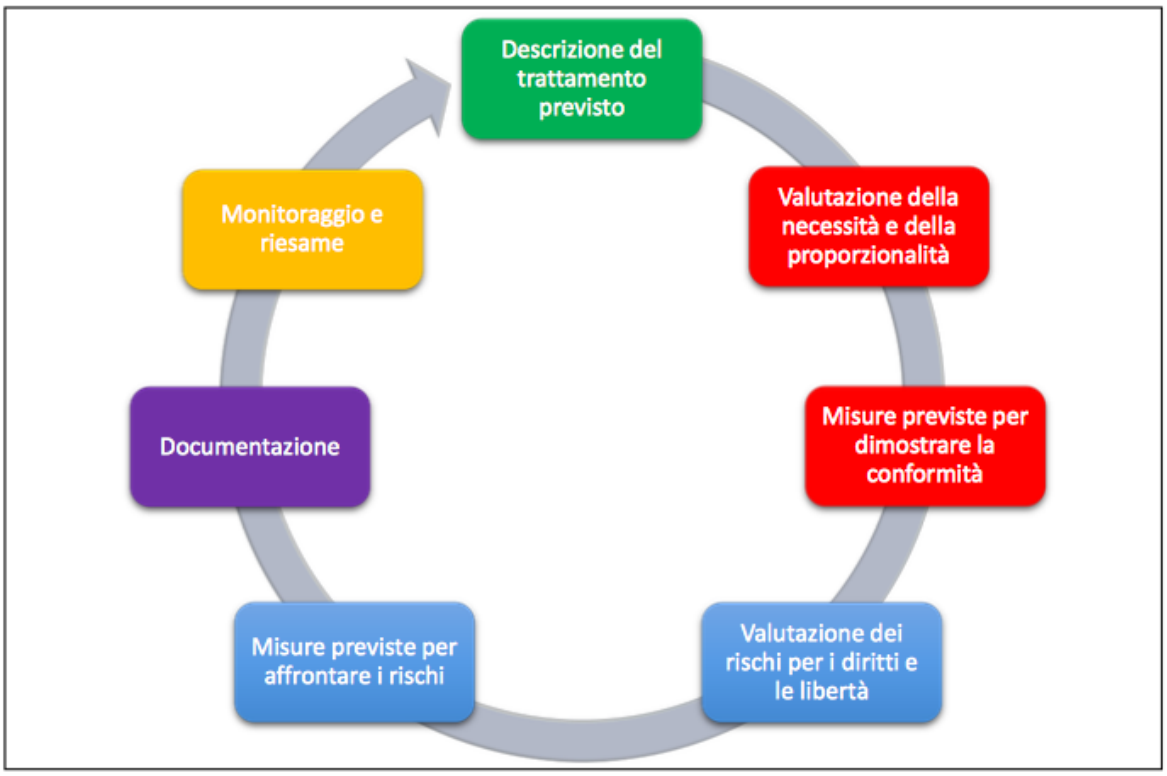
b) una **valutazione** della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una **valutazione dei rischi** per i diritti e le libertà 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 conformità 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 conformità al GDPR, è la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITÀ
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

SETTORE	SETTORE STAFF DEL SINDACO
SERVIZIO	Corpo di Polizia Locale
UFFICIO: denominazione e punti di contatto	Vigilanza territoriale
Titolare trattamento: denominazione e punti di contatto	Comune di Villamarzana Sindaco Daniele Menon
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di	Assistente della Polizia Locale Enrico Contiero, 0425938018 Interno 5, poliziamunicipale@comune.villamarzana.ro.it

contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	
Incaricati trattamento: denominazione e punti di contatto	- Paco Ghirotto - Enrico Contiero - Daniele Menon

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 68 - Le immagini video riprese dalle telecamere sono accessibili sia “in diretta” che a seguito di registrazione tramite apposito software installato su PC preposti. Tale software effettua un collegamento criptato con il sistema di videosorveglianza.
Mediante protocolli standardizzati di autenticazione è impedito l'accesso illecito. Ogni impianto di videosorveglianza è formato, oltre alla videocamera, di un box a doppia chiusura contenente un hard disk criptato nel quale vengono stoccati i dati delle videoregistrazioni. Automaticamente, e senza intervento umano, il sistema provvede alla cancellazione delle immagini registrate rendendo i dati irrecuperabili trascorsi 7 gg.

GDPR	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attività' amministrativa di cui all'art. 1, L. 241/1990 - **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 nonchè 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. 24.11.1981, n. 689 - D.Lgs. 30.04.1992, n. 285 (art. 116) - D.P.R. 16.12.1992, n. 495 - **D.L. 23/02/2009 n. 11**
Natura del trattamento	- Conferimento obbligatorio
Ambito di applicazione del trattamento	- Trattamento in ambito pubblico
Nome archivio/Banca dati	Sistema informativo relativo a sicurezza e ordine pubblico - base di dati e applicativo oggetto di comunicazione all'AGID, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca	- I dati sono registrati in archivi/banche di dati gestite con modalità elettroniche

dati	
Categorie-tipi di dati	- Dati idonei a rivelare l'origine razziale ed etnica - Dati relativi a comportamenti illeciti o fraudolenti - Dati idonei a rivelare l'appartenenza a categorie protette - Dati idonei a rivelare lo stato di gravidanza - Dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica - Dati idonei a rilevare la posizione di beni, strumenti, oggetti - Dati idonei a rilevare la posizione di persone - Dati idonei a rilevare immagini o suoni - Dati comuni identificativi
Luoghi di custodia dei dati	- In Italia presso le singole istallazioni di box atti alla videosorveglianza
Finalità del trattamento	Scheda n. 68 - Trattamento effettuato per finalità di ordine e sicurezza pubblica. I dati acquisiti vengono trattati esclusivamente per la finalità di gestione del processo/procedimento amministrativo e/o penale per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio. I dati possono essere trattati, altresì, per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalità di interesse pubblico	- Scheda n. 68 - Trattamento effettuato per rilevanti finalità' di interesse pubblico nella seguente materia: compiti di tutela della sicurezza pubblica, protezione civile, salvaguardia della vita e incolumità' fisica ai sensi dell'art. 2-sexies, comma 2 lett. u) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018.
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorità pubbliche, nell'esecuzione dei loro compiti, la condizione di liceità del legittimo interesse (in forza del quale il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) è 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 libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	- Trattamento ordinario dei dati - operazioni eseguite: c) altre operazioni indispensabili rispetto alla finalità del trattamento e diverse da quelle ordinarie quali la registrazione, la conservazione, la cancellazione o il blocco nei casi previsti dalla legge: consultazione, selezione estrazione ed archiviazione, raccolta di dati in luoghi pubblici o aperti al pubblico cancellazione immediata o nel breve periodo (massimo 7 giorni), distruzione. - Trattamento ordinario dei dati - operazioni eseguite: a) elaborazione in forma cartacea - Trattamento ordinario dei dati - operazioni eseguite: b) elaborazione con modalità informatizzate
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	COMANDO PROVINICALE CARABINIERI DI ROVIGO, STAZIONE CARABINIERI DI ARQUA' POLESINE, QUESTURA DI ROVIGO, COMANDO PROVINCIALE GUARDIA DI FINANZA DI ROVIGO
Categorie di trattamenti - particolari forme	N.R.

di elaborazione: ***diffusione***	
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***	nessuno
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	nessuno
Categorie di interessati	- Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Forze di Polizia –
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***	- Pc a disposizione del comando di Polizia locale del comune di Villamarzana
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***	- 7 giorni per i dati della videosorveglianza e, per eventuali altri dati, termine identificato in base alla normativa di settore o, comunque, in base al criterio della cancellazione immediatamente dopo il "periodo minimo indispensabile di trattamento dei dati"

categorie di dati	
Cessazione trattamento: ***modalità di cessazione dei dati***	- Eliminazione automatizzata da Hard disk contenente le immagini
Parere RPO/RTD	
Opinioni interessati o loro rappresentanti	
Rispetto codici di condotta approvati	
Adesione ad un meccanismo di certificazione	N.R.
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	

SEZIONE II
VALUTAZIONE DELLA NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITÀ AL GDPR
(art. 35, paragrafo 7, lettera b)

A) NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO

GDPR	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalità e necessità del trattamento in relazione alle finalità	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 e, in ogni caso, non superiore a 7 giorni come previsto dalla normativa applicabile. Vengono individuati soggetti espressamente preposti ed autorizzati all'accesso al luogo in cui sono conservati i monitor e i dati registrati È stato adottato un regolamento che disciplina le modalità di trattamento dei dati acquisiti con videosorveglianza

Misure che contribuiscono ai diritti degli interessati in relazione alle finalità	Comunicazione tramite apposito cartello che avverte della presenza di telecamere per la videosorveglianza per la pubblica sicurezza.

B) CONFORMITÀ GDPR

GDPR	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformità al GDPR	- Tracciabilità documentale del processo decisionale di gestione del rischio.

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

GDPR	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilità dei dati* (rilevati dalla prospettiva degli	- OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamità naturali - APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrità dei dati - CONTESTO: sottrazione/alterazione credenziali di autenticazione - 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)

interessati)	
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilità dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono più presenti sui sistemi del titolare né nella disponibilità dell'autore della violazione) - Furto di dati (i dati non sono più presenti sui sistemi del titolare ma nella disponibilità dell'autore della violazione) - Copia di dati (i dati sono ancora presenti sui sistemi del titolare ed anche nella disponibilità dell'autore della violazione) - Lettura di dati (presumibilmente i dati sono solamente stati visualizzati dall'autore della violazione)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati (rilevati dalla prospettiva degli interessati)	- Accessi esterni non autorizzati - Alterazione dolosa o colposa dati avvenuta internamente - Attacco Ransomware - Azione di virus informatici o di codici malefici - Carenza di consapevolezza, disattenzione o incuria - Comunicazione illegale dei dati e dei documenti - Copia abusiva - Degrado dei supporti e delle apparecchiature - Cortocircuito elettrico - Distruzione di apparecchiature o di supporti - Fenomeni meteorologici - Furto Apparecchiature - Incendio - Malfunzionamento hardware o software - Mancanza di continuità di alimentazione elettrica - Mancata manutenzione del sistema informativo - Perdita credenziali - Polvere, corrosione o gelo - Possibile rottura dell'hard disk o altri componenti hardware/software - Accessi tramite dispositivi mobili non autorizzati - Errato utilizzo doloso o colposo del software - Mancata distruzione o restituzione dei supporti raggiunta la finalità
PROBABILITÀ = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITÀ = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITÀ E GRAVITÀ (rilevata dalla prospettiva degli interessati)	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 **probabilità** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

1 = basso-trascurabile = è **molto improbabile** che la minaccia si possa verificare
2 = medio = è **improbabile** che la minaccia si possa verificare
3 = alto = = è **probabile** che la minaccia si possa verificare
4 = molto alto = è **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 **gravità**, 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 operatività ...).

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)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

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** atte a salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorità e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

GDPR	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-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 regolarità 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-10 - PROTEZIONE AREE E LOCALI: continuità dell'alimentazione elettrica - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- utilizzo 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) - Adozione di sistemi di videosorveglianza con sistema di allocazione dati autonomo, così da evitare utilizzo di server terzi. Tali sistemi di allocazione (hard disk) sono criptati, salvaguardati da doppia chiusura, e dotati di sistema di invio alert in caso di manomissione. Vengono inoltre utilizzati sistemi di videosorveglianza che inviano un flusso di dati criptato al server della Polizia Locale di Villamarzana. - 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'integrità delle informazioni rilevanti (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-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorità 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-05 - GESTIONE DATI: adeguate modalità di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: collaborazione di professionisti esterni per la gestione del rischio e la valutazione di impatto - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-22 - SISTEMA GESTIONE PRIVACY: registrazione delle consultazioni	
Misure di sicurezza:	- MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura	

procedurali	operativa per la gestione delle credenziali di autenticazione

C) RISCHIO RESIDUO

GDPR	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

GDPR	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

GDPR	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformità al GDPR	- La conformità giuridica al GDPR è 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 possibilità che il trattamento possa avere un rischio elevato nonché, in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attività e delle categorie di trattamento.

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

GDPR	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Attuate
Fasi attuazione misure	N.R.
Indicatori attuazione misure	- 100% di azioni attuate sul numero programmato
Responsabile attuazione misure	Sindaco

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

Videosorveglianza