Prot. 8696/2023 del 16/03/2023

Valutazione d'impatto sulla protezione dei dati personali - DPIA

ATTIVITA' DI TRATTAMENTO: Polizia locale - Trattamento relativo al videosorveglianza/sistemi di rilevazione delle immagini.

SETTORE: POLIZIA LOCALE

REFERENTE PRIVACY : COMANDANTE POLIZIA LOCALE

CRITERI PER DPIA – WP248: SI OBBLIGATORIA :

Monitoraggio sistematico;

Trattamento che ricade nell'Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679.

Redazione	Data	Elaborazione	Redazione
1	14/03/2023	Titolare del Trattamento – Sindaco pro-tempore	DPO Avv. Claudio Valente

SOMMARIO

1. NOZIONE DI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

2. QUADRO NORMATIVO

- REGOLAMENTO 2016/679/UE: Articoli 35 e 36
- Considerando C84, C89, C90, C91, C92, C93, C94, C95
- WP248 - 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
- Provvedimento Garante n. 467 dell'11.10.2018 – G.U. 269 del 19.11.2018

3. OBBLIGHI DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri, in base alle indicazioni della linea guida WP248:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

Tra l'altro il Garante ha pubblicato l'Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 – fra questi appunto ricade l'attività di Videosorveglianza, oggetto di tale valutazione.

4. METODO DI CONDUZIONE DELLA DPIA

Scopo dell'attività è quella di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento è conforme al regolamento GDPR e in seconda battuta comprendere se quel trattamento deve essere sottoposto ad una valutazione DPIA.

Il presente documento comprende, principalmente:

- una descrizione sistematica del trattamento previsto e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità del trattamento in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- 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 Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati.

In ossequio al principio del *data protection by design* il Titolare del Trattamento ha consultato il Responsabile della Protezione dei Dati circa:

- se condurre o meno la presente DPIA
- se condurre la DPIA con risorse interne o esternalizzandola
- quale metodologia adottare per la conduzione della stessa
- quali salvaguardie applicare per attenuare i rischi per i diritti e gli interessi delle persone interessate

Il Responsabile della Protezione dei Dati ha verificato la correttezza della conduzione della DPIA e sulla conformità alle normative vigenti delle conclusioni raggiunte.

5. VALUTAZIONE PRELIMINARE

5.1) FASE 1 - Descrizione del trattamento

Soggetti interessati

Utenti, cittadini.

Finalità del trattamento

- Funzioni di sicurezza urbana e controllo del patrimonio pubblico;
- Protezione Civile e altri eventi pubblici;
- Repressione dell'abbandono dei rifiuti
- Rilevazione infrazioni CdS e controlli della circolazione e del codice penale.

Descrizione del trattamento e flussi informativi

Il trattamento preso in considerazione è la raccolta e la conservazione (per un periodo di tempo limitato ad un massimo di 7 giorni), delle immagini relativamente all'impianto di videosorveglianza ubicato nel comune. Per ulteriori dettagli sul trattamento si rimanda al Regolamento Comunale sulla videosorveglianza aggiornato secondo le recenti disposizioni

Dati oggetto del trattamento

IMMAGINI (FOTOGRAMMI)
IMMAGINI (VIDEO)
DATI ELABORATI DA TARGHE VEICOLI

Modalità di trattamento

Di seguito si specificano le operazioni svolte:

- RACCOLTA DEI DATI (PRINCIPALMENTE AUTOMATIZZATA dai vari apparati)
- REGISTRAZIONE E CONSERVAZIONE (PRINCIPALMENTE AUTOMATIZZATA)
- ELABORAZIONE (TRAMITE PERSONALE ESPRESSAMENTE AUTORIZZATO)
- DISTRUZIONE/CANCELLAZIONE entro 7 giorni.

Operazioni eseguite

Raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione.

Conservazione dei dati trattati e risorse a supporto dei dati

I dati sono conservati in archivi elettronici e/o in archivi cartacei custoditi all'interno del Comando di Polizia Locale. Il Comando è dotato di idonee misure di sicurezza fisiche, tra le quali:

- Porte blindate;
- 2 hard disk interni

Processi interni coinvolti nel trattamento

Le principali aree/settori interni coinvolti nel trattamento sono:

- Polizia Locale

5.2) FASE 2 - Valutazione della conformità

Modalità di raccolta dei dati

Raccolta diretta presso l'interessato e/o acquisizione da altri soggetti.

Soggetti che hanno accesso ai dati

- Titolare del trattamento e soggetti espressamente individuati e autorizzati del Comando di Polizia Locale.
- Responsabili esterni del trattamento come individuati dall'Ente in ragione degli incarichi conferiti/dei servizi affidati.

È consentita la comunicazione dei dati ad altri soggetti pubblici e privati in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare a:

- Autorità Giudiziaria;

- Altre Forze di Polizia;
- Incaricati di indagini difensive proprie e altrui,; *consulenti della controparte;
- Eventuali Amministrazioni coinvolte o soggetti Pubblici;

Nello svolgimento delle proprie funzioni istituzionali l'Ente comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.

Modalità di trasferimento dei dati a soggetti terzi

In formato elettronico o cartaceo.

Modalità di conservazione aggiornamento e eliminazione dei dati

Le registrazioni video, a seconda della localizzazione delle telecamere, vengono conservate per 7 giorni presso la sala dedicata alla registrazione e conservazione delle immagini presente una stanza appositamente dedicata dalla Polizia Municipale del Comune di Sora.
Il Trattamento delle immagini (estrazione e consultazione) viene effettuato dal CED della Polizia Locale, su formale richiesta delle forze dell'ordine a cui vengono consegnate nella massima sicurezza.

IL TERMINE VIENE SOSPESO QUALORA RIGUARDI DEI PROVVEDIMENTI, O LE IMMAGINI VENGANO ACQUISITE DALLE AUTORITA' COMPETENTI PER EVENTI DANNOSI E/O ILLECITI.

I documenti cartacei riportanti dati non più occorrenti - se non protocollati e/o allegati in fascicolo - vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili.

Motivazione legittima per il trattamento (anche per categorie speciali di dati)/base giuridica del trattamento

Ex art. 6 comma 1 lettere C) D) E) F) del GDPR, ovvero:
- trattamento necessario per il perseguimento del legittimo interesse del titolare;
- salvaguardia interessi vitali dell'interessato (sia l'operatore che qualsiasi cittadino);
- trattamento necessario per adempiere ad un obbligo legale;
- trattamento necessario per svolgere un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;

Modalità di offerta di informativa agli interessati e di raccolta del consenso

Cartellonistica e segnaletica semplificata ai sensi art.14 del GDPR posizionata prima del raggio d'azione e in corrispondenza di ogni telecamera e resa ben visibile;
Pubblicata l'informativa estesa presso il sito web dell'ente nella relativa sezione privacy

Utilizzo per nuove/diverse finalità di dati personali già raccolti

Non è previsto

Modalità di verifica della accuratezza dei dati personali raccolti e trattati

Dati raccolti presso l'interessato.

Asset model a sostegno dei trattamenti

Hardware, software, archivi, reti.

Misure di sicurezza a garanzia della riservatezza dei dati / per prevenire trattamenti di dati personali non autorizzati o illegittimi

organizzative, quali: istruzioni interne; assegnazione di nomine al personale autorizzato; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative.
fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti. Trasferimento di dati in maniera sicura con il divieto di intrusione di nuovi dispositivi.
logiche, quali: identificazione dell'utente; controllo degli accessi a dati e programmi (con rilascio credenziali); monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione

Trasferimento di dati personali in un paese non facente parte dell'unione europea

Non è previsto

Diritti degli interessati

L'interessato ha diritto di chiedere al titolare del trattamento l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento; può inoltre opporsi al trattamento ed esercitare il diritto alla portabilità dei dati forniti e trattati in via automatizzata, con il consenso dell'interessato o sulla base di contratto stipulato fra le parti. I diritti riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
È diritto dell'interessato proporre reclamo avverso il trattamento dei dati operato dall'Ente alla competente Autorità di Controllo (Garante per la protezione dei dati personali), ovvero ricorso dinanzi all'Autorità Giudiziaria.

Il trattamento rispetta

- i principi di liceità, correttezza e trasparenza
- il principio di limitazione della finalità
- il principio di minimizzazione dei dati
- il principio di esattezza dei dati
- il principio di limitazione della conservazione dei dati
- il diritto di informazione
- il diritto di accesso ai dati
- il diritto di portabilità
- il diritto di rettifica
- il diritto di cancellazione (diritto all'oblio)
- il diritto di limitazione del trattamento
- il diritto di opposizione al trattamento

5.3) FASE 3 - CONDURRE LA DPIA?

Le risultanze della valutazione preliminare di anzi condotta non paiono evidenziare la sussistenza di rischi aventi particolare impatto su diritti e libertà delle persone i cui dati sono oggetto di trattamento. Peraltro, il trattamento in esame risulta essere posto in essere già precedentemente

all'entrata in vigore del Regolamento UE, sin dall'adozione da parte dello Stato italiano del Codice della Privacy, e da allora condotto sulla base dello stretto rispetto delle norme di riferimento in materia vigenti nel tempo (del resto, in gran parte coerenti con le nuove disposizioni europee), senza che si siano rilevati eventi dannosi nel periodo. Alla luce di tali considerazioni, si ritiene che eventuali rischi possano ritenersi sostanzialmente nel complesso **accettabili.**
In ogni caso, seppure il trattamento di cui si tratta non preveda neppure l'uso di nuove tecnologie, l'Ente - anche in considerazione della rilevante delicatezza dei dati trattati - ritiene comunque utile la conduzione di attività di miglior approfondimento della valutazione in questione.

Quindi, la tabella seguente illustra i principali rischi afferenti alla protezione dei dati, che si ritengono identificabili in fase di valutazione preliminare, correlati ad eventi relativi al contesto in cui si opera o relativi agli strumenti, oppure a comportamenti degli operatori:

Descrizione del rischio
1) Danneggiamento/ perdita/distruzione non autorizzata dati personali
2) Accesso non autorizzato dati personali
3) Trattamento non autorizzato (comprensivo di modifica, divulgazione……)
4) Trattamento non conforme alla finalità della raccolta o illecito

6. ESECUZIONE DPIA

6.1) Fase 1 - Informazioni integrative per analisi del rischio

(in aggiunta a quanto già esposto in sede di valutazione preliminare, cui si rimanda)

Tecnologie utilizzate

Non verranno utilizzate nuove tecnologie informatiche che potrebbero avere un significativo potenziale di violazione della protezione dei dati personali e riduzione del livello di protezione dei dati, che bisogna garantire agli interessati

Metodi di identificazione

Non verranno utilizzati nuovi metodi di identificazione e di automatizzazione dei dati.

Coinvolgimento di altre strutture

L'iniziativa di trattamento non coinvolge altre strutture.

Modifiche alle modalità di trattamento dei dati

L'iniziativa di trattamento non apporterà nuove o significative modifiche alle modalità di trattamento dei dati personali, che potrebbero destare preoccupazioni nell'interessato.
I dati personali, afferenti all'interessato, già presenti in un esistente data base, non verranno assoggettati a nuove o modificate modalità di trattamento.
L'iniziativa di trattamento non apporterà nuove o significative modifiche alle modalità di consolidamento, interscambio, riferimenti incrociati, abbinamento di dati personali, provenienti da più sistemi di trattamento.

Modifiche alle procedure di trattamento dei dati

Il trattamento non potrà introdurre nuove modalità e procedure di raccolta dei dati, che non siano sufficientemente trasparenti o siano intrusive, né modifiche a sistemi e processi, appoggiati a

normative in vigore, che possano avere esiti non chiari o non soddisfacenti, o che modifichino il livello di sicurezza dei dati, in modo da portare ad esiti non chiari o non soddisfacenti.
Il trattamento non potrà introdurre nuove o modificate procedure sicure di accesso ai dati o modalità di comunicazione e consultazione, che possano essere non chiare o permissive.
Il trattamento non introdurrà nuove o modificate modalità di conservazione dei dati, che possano essere non chiare o prolungate oltremodo.

Esenzioni dalla applicazione delle disposizioni del regolamento

L'attività di trattamento non esula dall'ambito delle disposizioni legislative dell'unione europea, non è svolto da una persona fisica esclusivamente per fini personali e familiari e non è svolta da autorità pubbliche al fine di prevenzione, indagine, individuazione e perseguimento di reati o al fine di applicare pene.

6.2) Fase 2 - Valutazione del rischio

a) metodologia di valutazione
L'analisi del rischio è un processo per identificare e valutare il danno causabile da minacce e vulnerabilità in combinazione su uno o più asset ben precisi. Serve inoltre a giustificare le contromisure, a valutare che siano efficaci, di costo ragionevole, effettivamente applicabili al contesto e in grado di rispondere in tempo alle minacce. Tale analisi ha come obiettivo minimizzare la probabilità di accadimento dei rischi e gli impatti che possibili violazioni dei dati personali potrebbero comportare agli individui, come di seguito esemplificativamente sintetizzati:
Rischi: distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato ai dati personali.
Impatto:
- da violazione della sicurezza fisica
- da violazione dei dati di identificazione o attinenti l'identità personale
- materiale (perdite finanziarie o al patrimonio)
- morale o biologico (turbamento per la diffusione di una notizia riservata, compromissione di uno stato salute, evento lesivo di diritti umani o integrità della persona)
- sociale (conseguenze di tipo discriminatorio, perdite di autonomia)

La DPIA si basa su un'analisi dei rischi centrata su
- rischi derivanti da contenuto intrinseco del trattamento
- rischi derivanti da possibili violazioni di sicurezza

In relazione ai possibili controlli applicabili, ricavando, così, un **indice di rischio "normalizzato"** rispetto al contesto in esame.

Il rischio normalizzato RN viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, V)
dove:

P = probabilità (stima della probabilità di accadimento degli eventi che causano la perdita, violazione, distribuzione non controllata di dati = **pericoli**)

C = conseguenze generate dall'evento (stima della gravità dei danni attesi rispetto all'accadimento di un determinato evento)

V = vulnerabilità rispetto al grado di adeguatezza delle misure (grado di adeguatezza delle misure che contrastano il manifestarsi degli eventi)

In prima battuta viene ricavato il **rischio intrinseco Ri** come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla probabilità P è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle conseguenze C è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

La **matrice** che scaturisce dalla combinazione di probabilità e conseguenze è rappresentata in figura seguente:

PROBABILITA'	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	$(1 \leq Ri \leq 2)$
Basso	$(3 \leq Ri \leq 4)$
Rilevante	$(6 \leq Ri \leq 9)$
Alto	$(12 \leq Ri \leq 16)$

Per ricavare il **Rischio Normalizzato RN**, viene introdotto il fattore Vulnerabilità che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla vulnerabilità V è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		VALORE
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

□ **0,25;** □ **0,5;** □ **1.**

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

VULNERABILITA'	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		RISCHIO INTRINSECO			

RISCHIO NORMALIZZATO	
RN = Ri x V	Valori di riferimento
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

b) definizione di aree di pericolo, rischi generati e valutazione del livello di rischio intrinseco

Di seguito la suddivisione delle principali aree di pericolo con i rischi generati, e le relative stime su probabilità di accadimento e conseguenze:

Rischio intrinseco *(valutato sulla base della media dei valori peggiori di probabilità e conseguenza stimati per rischio specifico)*

• RISCHIO 1: Danneggiamento / Perdita / Distruzione non autorizzata		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante (2*4=8)
• RISCHIO 2: Accesso non autorizzato		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante (2*4=8)
• RISCHIO 3: Trattamento non autorizzato		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante (2*4=8)
• RISCHIO 4: Trattamento non conforme alla finalità della raccolta o illecito		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante (2*4=8)

c) valutazione dell'idoneità delle misure di sicurezza tecniche e organizzative a rendere il rischio accettabile

TRATTAMENTO **CON** L'AUSILIO DI STRUMENTI ELETTRONICI

Rischio	**Misure**	**Idoneità**
RISCHIO 1) danneggiamento, distruzione o a perdita del dato	- aggiornamento annuale dei programmi per elaboratore (semestrale per trattamento di dati sensibili o giudiziari) - effettuazione di backup full dei database dei gestionali giornalieri conservando gli ultimi 7 - dotazione di impianti antincendio - presenza di almeno un alimentatore - utilizzo di infrastrutture servite da alimentazione privilegiata (gruppo elettrogeno) - stanza riservata alla registrazione delle immagini della videosorveglianza.	ADEGUATE
RISCHIO 2) Accesso non autorizzato (ai locali, al sistema ed ai dati)	- i server sono collocati in locali chiusi a chiave (porte blindate), con una piccola finestra - i supporti rimovibili vengono custoditi in luogo non accessibile a persone diverse dalle autorizzate - assegnazione di credenziali di accesso alla rete differenziate per servizio/gestionale e di password personalizzate - adozione di sistema di gestione degli utenti che associa il data base degli stessi con le rispettive autorizzazioni, disponibile centralmente in rete al fine di un eventuale recupero su richiesta dei soggetti autorizzati al trattamento dei dati - utilizzo di salvaschermo protetti da password in caso di inattività -	ADEGUATE
RISCHIO 3) trattamento non autorizzato	- ogni incaricato del trattamento è munito di credenziali di autenticazione e/o parola chiave; è operativa la procedura che ne consente l'autonoma sostituzione periodica da parte del singolo operatore - di norma il codice identificativo personale fornito ad ogni operatore non viene assegnato a persone diverse; - i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persona diversa dall'incaricato del trattamento - i dati non devono essere condivisi, comunicati o	ADEGUATE

	inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative	
RISCHIO 4) trattamento non conforme alla finalità della raccolta o illecito	- è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, dati non più occorrenti vengono di norma cancellati o distrutti (anche facendone richiesta all'Amministratore di Sistema, ove il soggetto responsabile non fosse in possesso delle necessarie abilitazioni); qualora fossero conservati, non sono comunque utilizzabili.	ADEGUATE

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Rischio	Misure	Idoneità
accesso non autorizzato	- la conservazione dei documenti contenenti dati personali e/o sensibili avviene in archivi ad accesso selezionato e controllato; i locali in cui sono conservati tali documenti devono essere chiusi al termine dell'orario di lavoro - i documenti contenenti dati sensibili, se affidati all'incaricato del trattamento, devono da questo essere conservati in modo tale da non garantire a terzi la consultabilità degli stessi fino alla restituzione all'archivio d'ufficio - l'accesso agli archivi non è consentito dopo l'orario di chiusura degli stessi, coincidente con l'orario di chiusura degli uffici o con l'effettivo termine delle attività lavorative. Peraltro, qualora si renda necessario consentire l'accesso agli archivi dopo l'orario di chiusura degli stessi, occorre prevedere procedure di controllo e di identificazione e registrazione dei soggetti ammessi, fatte salve preventive autorizzazioni - i documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro - fare attendere soggetti estranei in luoghi in cui non siano presenti informazioni riservate o dati personali; se per ragioni di lavoro gli stessi possono accedere agli uffici, avere cura di riporre eventuali documenti e se necessario di attivare il salvaschermo dei p.c. - evitare l'esportazione di dati personali e/o l'installazione degli stessi su attrezzature diverse da quelle messe a disposizione dall'Ente (ad es. computer di casa)	ADEGUATE

trattamento non autorizzato	- il personale che tratta i dati è opportunamente nominato come autorizzati al trattamento dei soli dati la cui conoscenza sia strettamente necessaria per lo svolgimento dell'incarico affidato o per l'espletamento delle competenze attribuite alla struttura organizzativa di riferimento - divieto di richiedere, raccogliere e/o conservare in fascicolo dati personali non pertinenti con le competenze e le attività svolte o eccedenti le necessità istruttorie delle attività assegnate - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative - il trasporto di dati personali all'esterno dei locali ove si svolge il trattamento, ma comunque all'interno dell'Ente avviene in modo da garantirne la riservatezza	ADEGUATE
trattamento non conforme alla finalità della raccolta o illecito	- è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, i documenti riportanti dati non più occorrenti - se non protocollati e/o allegati in fascicolo - vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili. - i supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di un eventuale riutilizzo; se ciò non è possibile devono essere distrutti	ADEGUATE

d) valutazione rischio normalizzato **(sulla base del valore peggiore assegnato alle misure di sicurezza relativamente al rischio specifico).**

• **RISCHIO 1: Danneggiamento / Perdita / Distruzione non autorizzata**		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	**BASSO**

• **RISCHIO 2: Accesso non autorizzato**		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	**BASSO**

• **RISCHIO 3: Trattamento non autorizzato**		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	***BASSO***

• **RISCHIO 4: Trattamento non conforme alla finalità della raccolta o illecito**		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	**BASSO**

7. Risultati DPIA

A valle dell'indagine DPIA condotta l'attività ricade in **fascia BASSA.**

In **appendice** sono illustrati in sintesi tutti i rischi identificati e le opzioni che permettano di mitigare, evitare o mettere sotto controllo questi stessi rischi, con evidenza del grado di rischio normalizzato.
Si dà inoltre conto della previsione di ulteriori possibili misure di sicurezza tecniche e organizzative atte ad assicurare un ancor maggiore contenimento dei rischi, in via di implementazione o di prossima attuazione.
Si uniscono per completezza di informazione le misure di tutela della privacy nell'esercizio della professione sanitaria e delle attività correlate, adottate allo scopo di prevenire e/o limitare violazioni della riservatezza.

8. Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati

Secondo le buone prassi, è opportuno che la presente valutazione d'impatto venga riesaminata periodicamente, e particolarmente quando nell'intervallo di tempo trascorso dal completamento della DPIA si siano verificate delle modifiche nei rischi connessi al trattamento o vengano messe in evidenza delle anomalie.
A seguire alcuni esempi di modifiche alle attività di trattamento, rischi connessi e cambiamenti nel contesto organizzativo o sociale che debbono indurre ad una revisione della DPIA:
- Cambiamento sulle attività di trattamento, in termini di:

- Contesto o finalità del trattamento,
- Tipologia di dati personali trattati
- Destinatari o modalità di raccolta dei dati personali
- Combinazioni di dati provenienti da fonti differenti
- Trasferimento di dati all'estero

- Modifica ai rischi con impatto sui diritti degli interessati derivati da:

- Presenza di nuove minacce
- Modifica ai sistemi informativi a supporto del trattamento
- Soppressione di contromisure esistenti
- Nuovi scenari di rischio
- Nuovi potenziali impatti sulle dimensioni di analisi (Riservatezza, Integrità, Disponibilità)
- Attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali.

Inoltre, si rende comunque necessaria una revisione della DPIA tutte le volte che si è in presenza di mutamenti nel contesto organizzativo o sociale per il trattamento in essere.

Firma Titolare del Trattamento dei Dati:

Il Sindaco del Comune di Sora Dott. Luca Di Stefano

Firma del DPO: Avv. Claudio Valente

8. Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati

Secondo le buone prassi, è opportuno che la presente valutazione d'impatto venga riesaminata periodicamente, e particolarmente quando nell'intervallo di tempo trascorso dal completamento della DPIA si siano verificate delle modifiche nei rischi connessi al trattamento o vengano messe in evidenza delle anomalie.
A seguire alcuni esempi di modifiche alle attività di trattamento, rischi connessi e cambiamenti nel contesto organizzativo o sociale che debbono indurre ad una revisione della DPIA:
- Cambiamento sulle attività di trattamento, in termini di:

- Contesto o finalità del trattamento,
- Tipologia di dati personali trattati
- Destinatari o modalità di raccolta dei dati personali
- Combinazioni di dati provenienti da fonti differenti
- Trasferimento di dati all'estero

- Modifica ai rischi con impatto sui diritti degli interessati derivati da:

- Presenza di nuove minacce
- Modifica ai sistemi informativi a supporto del trattamento
- Soppressione di contromisure esistenti
- Nuovi scenari di rischio
- Nuovi potenziali impatti sulle dimensioni di analisi (Riservatezza, Integrità, Disponibilità)
- Attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali.

Inoltre, si rende comunque necessaria una revisione della DPIA tutte le volte che si è in presenza di mutamenti nel contesto organizzativo o sociale per il trattamento in essere.

Firma Titolare del Trattamento dei Dati:

Il Sindaco del Comune di Sora Dott. Luca Di Stefano

Firma del DPO: Avv. Claudio Valente