Valutazione d'impatto sulla protezione dei dati
ai sensi dell'art. 35 del GDPR 2016/679

Indice

Quando eseguire una Valutazione d'impatto sulla protezione dei dati

La Dpia – Data Protection Impact Assesment – è una procedura prevista dall'articolo 35 del Regolamento (UE) 2016/679.

La valutazione d'impatto della protezione dei dati (DPIA) serve a descrivere un trattamento di dati per valutarne la necessità, la proporzionalità e i relativi rischi.

L'obiettivo è quello di stabilire misure idonee ad affrontare i rischi in riferimento ai diritti e alle libertà delle persone fisiche di cui si effettua il trattamento dei dati.

Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

L'art. 35 prevede una specifica valutazione di impatto quando i trattamenti, considerate le circostanze indicate nella norma, possono presentare rischi elevati per gli interessati e ne specifica i casi in cui è necessaria e ne procedimentalizza anche le modalità da seguire e gli elementi da tenere in considerazione.

Nello specifico, la valutazione di impatto *"è richiesta in particolare nei casi seguenti:*

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; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

L'art. 35 prevede inoltre un ruolo molto rilevante delle Autorità di controllo che possono redigere e rendere pubblico un elenco delle tipologie di trattamenti per i quali è richiesta comunque la valutazione di impatto (art. 35, 4); così come possono, se lo ritengono opportuno, redigere un elenco delle tipologie di trattamenti per i quali essa non è necessaria.

L'art. 36, poi, stabilisce la consultazione preventiva obbligatoria dell'Autorità di controllo quando il titolare ritiene che i trattamenti richiedano misure specifiche per attenuarne i rischi.

È inoltre utile precisare che nelle linee-guida in materia di valutazione d'impatto sulla protezione dei dati[1] il WP29[2] raccomanda di effettuare comunque la DPIA in tutti i casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.

Inoltre, sempre il WP29 nelle predette linee guida per la determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 ha precisato che:

"come indicato dalle parole "in particolare" nella frase introduttiva dell'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo. Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati. Anche tali trattamenti devono essere

---

[1] 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 il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.

[2] Gruppo dell'articolo 29 per la tutela dei dati (in inglese Article 29 Working Party o WP29) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Oggi diventato European Data Protection Board (Comitato europeo per la protezione dei dati) col nuovo Regolamento europeo ha sostituito il Gruppo di lavoro articolo 29

soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati. Per questo motivo, i criteri sviluppati qui di seguito vanno, talvolta, al di là di una semplice spiegazione dell'interpretazione dei tre esempi di cui all'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati."

È poi necessario considerare che il Garante per la protezione dei dati personali italiano, circa i criteri che un Titolare deve considerare per determinare se è necessario eseguire una valutazione di impatto (DPIA), si è espresso nel seguente modo:

"Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l'autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

Si tratta di uno degli elementi di maggiore rilevanza del vigente quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati.

I titolari sono infatti tenuti non soltanto a garantire l'osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

Le stesse linee guida del WP29 precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all'art. 35), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.

Le linee-guida chiariscono, peraltro, anche quando una valutazione di impatto non sia richiesta: ciò vale, in particolare, per i trattamenti in corso che siano già stati autorizzati dalle autorità competenti e non presentino modifiche significative prima del 25 maggio 2018, data di piena applicazione del regolamento.

In sostanza le linee-guida indicano è che la valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri. In questo senso, la valutazione di impatto permette di realizzare concretamente l'altro fondamentale principio fissato nel regolamento 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (data protection by design) di qualsiasi trattamento."

I criteri specifici individuati dal WP29 per determinare quando la DPIA è obbligatoria sono:

– trattamenti valutativi o di scoring, compresa la profilazione;

– **processo decisionale automatizzato** che ha effetto giuridico o incide in modo analogo significativamente quindi decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);

– **monitoraggio sistematico (es: videosorveglianza)** che include i trattamenti utilizzati per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c)). Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro

dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

– **dati sensibili o dati aventi carattere altamente personale**, questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli degli indagati. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;

– **trattamenti di dati personali su larga scala**, il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

a) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

b) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

c) la durata, ovvero la persistenza, dell'attività di trattamento;

d) la portata geografica dell'attività di trattamento;

– creazione di corrispondenze o combinazione di insiemi di dati, combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);

– **dati relativi a interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati è un criterio che causa un aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

– **utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.)**;
– trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).
La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.
Sempre il WP29 definisce la DPIA non è necessaria per i trattamenti che:

– non presentano rischio elevato per diritti e libertà delle persone fisiche;
– hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
– sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
– sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
– fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

Conclusioni circa la necessità di effettuare la DPIA nel caso di specie
Alla luce della disamina di quanto disposto dal Regolamento (UE) 2016/679 all'articolo 35 e di quanto chiarito sia dal Garante della Protezione dei dati personali italiano e a livello UE dal Gruppo dell'articolo 29 è da ritersi necessario effettuare una valutazione di impatto (DPIA) circa il rischio elevato per i diritti e le libertà delle persone fisiche che può presentare l'adozione di dispositivi elettronici per la rilevazione di violazioni al Codice della strada per i motivi esposti di seguito.
Il Garante per la Protezione dei Dati Personali con il Provvedimento in materia di Videosorveglianza dell'8 aprile 2010 al **punto 5.3.** ha definito le modalità e le procedure di trattamento assimilando in tutto e per tutto gli impianti elettronici di rilevamento automatizzato delle infrazioni ai sistemi di videosorveglianza.
Orbene, prendendo in considerazione i criteri definiti dal Gruppo dell'articolo 29 per determinare l'obbligatorietà della realizzazione della DPIA pare indiscutibile che, nel caso di adozione di dispositivi elettronici di rilevamento automatizzato delle infrazioni, siano rilevabili "almeno due di questi criteri" potendosi compiere con tali dispositivi:

1. un processo decisionale automatizzato;
2. un monitoraggio sistematico;
3. di dati sensibili o dati aventi carattere altamente personale;
4. su larga scala;
5. che possono comprendere anche dati relativi a interessati vulnerabili;
6. e che potrebbero comprendere utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative.

Dati e Valutatori

Ente: Comune di Ferentino

Sezione: Valutazione sul sistema di videosorveglianza cittadino

Autore dell'Analisi: Avv. Piergianni Fiorletta

DPO Comune Ferentino: Dott. Massimo Genovesi

DPO Comune Ferentino: Stato Valutazione 100%

- Validazione Analisi dei rischi

- Validazione Piano d'azione

Principi fondamentali

Piano d'azione/misure correttive:

Devono essere nominati Responsabili del trattamento:

- la ditta che effettua la manutenzione dei dispositivi elettronici;
- la ditta che effettua la manutenzione del software;
- tutti i soggetti esterni che svolgono operazioni relative al trattamento dei dati ai fini manutentivi.

Misure esistenti o pianificate

Piano d'azione/misure correttive:
Devono essere stipulati gli atti di nomina dei responsabili del trattamento (Società in outsourcing) che definiscano puntualmente oggetto, durata, finalità del trattamento e obblighi delle parti contraenti. In particolare, il contratto deve contenere, disposizioni relative a:
- gli obblighi dei responsabili in materia di riservatezza dei dati personali affidati;
- requisiti minimi di autenticazione degli utenti;
- clausole in materia di restituzione e/o distruzione dei dati allo scadere del contratto;
- regole per la gestione e la notifica di eventuali incidenti.

Rischi

Nessun piano d'azione registrato.

Validazione

DPO e parere degli interessati

Nome del DPO/RPD

Dott. Massimo Genovesi

Parere del DPO/RPD

Seppure il tipo di trattamento in sé possa rappresentare un rischio relativo ai diritti e libertà dei soggetti interessati qualificabile come elevato, si ritiene che i dispositivi e le misure tecniche ed organizzative individuate e adottate fin dalla progettazione e che saranno utilizzate durante l'esercizio siano adeguate a mitigare il rischio portando il rischio residuale ad un livello che può essere qualificato come residuale basso

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si ritiene utile per questo trattamento richiedere il parere degli interessati in quanto è un trattamento finalizzato a limitare e reprimere comportamenti illeciti. La base giuridica del trattamento eseguito, ai sensi dell'art. 6, comma 1, lettera e) del Reg. UE 2016/679 è rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Trattamento dati da riprese video, audio, fotogrammi nell'ambito divarie attività dell'ente, nel dettaglio:

- ✓ videosorveglianza ("fissa") con funzioni di sicurezza urbana, tutela del patrimonio pubblico e di protezione dei dati personali e dei sistemi informativi
- ✓ sicurezza e polizia giudiziaria
- ✓ sistema di fototrappole per abbandono rifiuti (videosorveglianza mobile)
- ✓ sicurezza stradale e monitoraggio del traffico veicolare
- ✓ vigilanza e prevenzione reati ed illeciti ambientali

Questa DPIA è atta alla valutazione dell'impatto connesso all'uso di nuove tecnologie al fine di rilevare immagini catturate attraverso l'utilizzo di fototrappole per poi poter comminare sanzioni amministrative contro l'abbandono illegittimo dei rifiuti nelle periferie del comune di Ferentino nonché per la tutela della pubblica sicurezza, prevenzione e accertamento di reati.

Nella presente DPIA sono presi in considerazione anche i trattamenti di dati personali operati per mezzo di tecnologie che permettono la rilevazione di filmati/immagini degli interessati nonché numero di targhe di veicoli con i quali vengono abbandonati illegittimamente i rifiuti nelle aree di proprietà del comune di Ferentino.

Si rileva che la gestione di risorse locali è di norma a carico dell'amministrazione che deve anche curare gli aspetti relativi alla sicurezza informatica anche se il fornitore dei servizi locali potrà essere coinvolto comunque come responsabile esterno del trattamento.

Le soluzioni in cloud, da privilegiare secondo le linee guida per l'informatica nella PA, sono a loro volta caratterizzate da elevati rischi che devono comunque essere gestiti in collaborazione con il fornitore del servizio, da scegliere fra quelli abilitati secondo la circolare AGID n. 2 del 9 aprile 2018, che assumerà il ruolo di responsabile esterno del trattamento.

Le operazioni di trattamento dati che il Comune di Ferentino esegue sul territorio attraverso i diversi sistemi di videosorveglianza, perseguono le seguenti finalità: vigilanza sulla sicurezza stradale e della mobilità veicolare e pedonale; svolgimento di funzioni di pubblica sicurezza; vigilanza e prevenzione reati ed illeciti ambientali; attività di polizia giudiziaria.

L'attività di videosorveglianza eseguita dal Comune di Ferentino è esercitata per lo svolgimento di funzioni e poteri pubblici ed il raggiungimento delle finalità istituzionali come sopra rappresentate e precisate, consentendo quindi di garantire ai cittadini il rispetto delle regole civili, penali ed amministrative nonché di civile educazione che consentono la normale convivenza e coabitazione nella condivisione di uno spirito di reciproco rispetto e di rispetto

delle Istituzioni e delle loro funzioni. I sistemi di videosorveglianza utilizzati dal Comune di Ferentino sono, infatti, proporzionati ed efficaci rispetto alle finalità prefissate e sono tali da non comportare rischi ultronei rispetto a quelli inseriti in un contesto di normale funzionalità dei sistemi tecnologici delle tipologie in uso, avuto anche riguardo alla utilizzazione dei medesimi strumenti anche in altri contesti urbani, considerazione questa che consente di accrescere la fiducia e la credibilità degli strumenti stessi. Gli strumenti tecnologici in uso sono i seguenti: 1) sistema di videosorveglianza con telecamere fisse posizionate agli accessi all'area urbana e nel territorio, finalizzata al presidio del territorio stesso nonché alla vigilanza del traffico veicolare e pedonale, anche con dispositivi idonei alla lettura targhe; 2) sistema di videosorveglianza ambientale con "fototrappole" amovibili posizionate in prossimità dei luoghi destinati al gettito di rifiuti ovvero in aree presso le quali è stato rilevato ovvero potrebbe verificarsi il gettito irregolare e abusivo di rifiuti.

Quali sono le responsabilità connesse al trattamento?

La complessità delle azioni e dei possibili risvolti in termini di violazione della privacy implica una collaborazione fattiva tra le varie parti in causa. Queste sono, in particolare:

1. il **Titolare del trattamento**: il Comune di Ferentino, rappresentato ai fini previsti dal GDPR dal Sindaco *pro tempore*, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").

2. Il Titolare è responsabile dell'osservanza dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di PEG, previa apposita analisi preventiva della situazione in essere, tenuto conto dei corsi d'attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

4. Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso

lo stesso interessato;

b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35,GDPR, considerando la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

6. Il Titolare, inoltre, provvede a:

a) designare i "Delegati al trattamento" nelle figure dei Dirigenti/Responsabili P.O. e dei Funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;

b) nominare il Responsabile della protezione dei dati;

c) nominare quale Responsabile (esterno) del trattamento i soggetti pubblici e privati affidatari di attività e servizi per conto dell'Amministrazione comunale anche relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

Autorizzato (interno) al trattamento:

1. In relazione alle dimensioni organizzative del Comune, sono designati "Autorizzati al trattamento" i Dirigenti dei settori in cui si articola l'organizzazione comunale, in quanto in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative volte a garantire che i trattamenti siano effettuati in conformità al GDPR.

2. I soggetti "Autorizzati al trattamento" provvedono, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti loro affidati dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvedono:

- a collaborare alla gestione del registro delle attività di trattamento del Comune;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantirela sicurezza dei trattamenti;
- collaborare alle richieste di accesso, di limitazione ed opposizione degli interessatirelative a trattamenti di dati personali;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamentied alle

connesse attività di controllo;

- ad assistere il Titolare nella conduzione della valutazione dell'impatto sullaprotezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogniinformazione di cui è in possesso;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

3. I soggetti "Autorizzati al trattamento", sono designati, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi ed i diritti del Titolare del trattamento.

4. I soggetti "Autorizzati al trattamento", possono altresì designare altri soggetti "Incaricati al trattamento dei dati personali", identificandoli nei Titolari di P.O., nei Responsabilidi Servizio e nei collaboratori, ciascuno per il proprio ambito operativo.

Responsabili (esterni) del trattamento:

1. I Responsabili esterni del trattamento sono le persone fisiche, giuridiche, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo esterno all'Amministrazione comunale che possono essere nominati - dal "Responsabile al trattamento" e previa autorizzazione scritta da parte del Titolare - su un determinato trattamento attenendosi, nelle operazioni svolte, alle istruzioni ricevute.

2. Detti soggetti, in qualità di Responsabili esterni del trattamento, devono fornire le garanzie di cui al precedente art. 3 attraverso la stipulazione di atti/contratti in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del Responsabile del trattamento e le modalità di trattamento.

3. Gli atti di cui innanzi devono in particolare contenere quanto previsto dall'art. 28, p. 3,GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

Più in generale il Titolare del trattamento è soggetto alle seguenti norme di riferimento:

Norma	Titolo della fonte	Descrizione
Regolamento (UE) 2016/679	Regolamento (UY) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati - RGPD)	Norma UE (regolamento) di riferimento per quanto riguarda il trattamento dei dati personali
D.Lgs. 196/2003	Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE	Norma nazionale di riferimento per quanto riguarda il trattamento dei dati personali.
Direttiva (UE) 2016/680	Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;	Norma UE (direttiva) di riferimento per quanto riguarda il trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
D.Lgs. 51/2018	Decreto Legislativo 18 maggio 2018, n. 51 – Attuazione della Direttiva UE 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";	Norma nazionale di adattamento della direttiva UE per quanto riguarda il trattamento dei dati personali.
DPR del 15/01/2018	Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di	Regolamento sulle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia.

	polizia, da organi, uffici e comandi di polizia"	
Art. 54, D.Lgs. 267/2000	Decreto Legislativo 18 agosto 2000, n. 267 Testo unico delle leggi sull'ordinamento degli enti locali.	Attribuzioni del sindaco nelle funzioni di competenza statale
D.L. 23 febbraio 2009, n. 11,	Convertito con modificazioni dalla L. 23 aprile 2009, n. 38	Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori ", ed in particolare dall'art. 6;
Prov. GPDP n. 1712680, 08/04/2010	Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);	Provvedimento del Garante della Protezione dei dati personali in materia di videosorveglianza
Linee Guida EDPB 3/2019	Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati (European Data Protection Board);	Linee guida dell'European Data Protection Board sul trattamento dei dati personali attraverso dispositivi video
Le linee guida 07/2020	Le linee guida 07/2020 sui concetti di titolare e responsabile nel General Data Protection Regulation.	Le linee guida 07/2020 sui concetti di titolare e responsabile nel General Data Protection Regulation, Adottate il 07 luglio 2021, dal Comitato Europeo per la produzione dei dati
Art. 13 Legge 163/2017	Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017.	Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
LEGGE 18 aprile 2017, n. 48	Conversione in legge, con modificazioni, del decreto-legge 20 febbraio 2017, n. 14	Disposizioni urgenti in materia di sicurezza delle città.
Provvedimenti e codici di deontologia promossi dal Garante per la protezione dei dati personali	Le linee guida 3/2019	Trattamento dei dati personali attraverso dispositivi video, adottate il 29 gennaio 2020
"	Provvedimento a carattere Generale del 29\11\2000:	Videosorveglianza – Il decalogo delle regole per non violare la Privacy.
"	Provvedimento a carattere Generale del 29\04\2004	Videosorveglianza – Provvedimento generale.

"	Provvedimento in materia di Videosorveglianza del 8/4/2010.	Videosorveglianza – Provvedimento generale.
Circolare del Ministero dell'Interno	dell'8 febbraio 2005, n. 558/A/471 e s.m.i	Videosorveglianza
Circolare del Ministero dell'Interno	del 6 agosto 2010, n. 558/A/421.2/70/195960	Videosorveglianza
Direttive del Ministero degli Interni avente oggetto	n. 558/SICPART/421.2/70 del 02 marzo 2012 e s.m.i.	Sistemi di videosorveglianza in ambito comunale
Circolare n. 2/2017 del 18 aprile 2017 (Agenzia per l'Italia Digitale)	in sostituzione della circolare 1/2017 del 17 marzo 2017	Misure minime di sicurezza ICT per le pubbliche amministrazioni" (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015" (GU 103 del 05/05/2017)
Sentenza del TAR Campania n. N. 02608/2023	REG.PROV.COLL. N. 00253/2023 REG.RIC.	Accesso agli atti

Ci sono standard applicabili al trattamento?

Attualmente non sono stati rinvenuti standard, certificazioni o codici di condotta applicabili al caso in esame per la videosorveglianza

Valutazione: Accettabile

DATI, PROCESSI E RISORSE DI SUPPORTO

Quali sono i dati trattati?

I dati trattati consistono in immagini e video registrati sul piano operativo; la registrazione è attiva sulle 24 ore e le immagini registrate vengono salvate solamente dal personale incaricato qualora vi sia una situazione di particolare criticità che necessita la documentazione video degli eventi.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il trattamento dei dati personali è effettuato a seguito dell'attivazione di tutti gli impianti/sistemi/presidi di video-sorveglianza installati sul territorio cittadino.

La disponibilità tempestiva di immagini presso la Sala Operativa della Polizia Locale costituisce uno strumento di prevenzione e di razionalizzazione dell'azione delle pattuglie dislocate sul territorio comunale, anche in raccordo con altre Forze dell'Ordine; attraverso tali strumenti l'Ente persegue l'intento di tutelare la popolazione ed il patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.

A tal fine il Comune, previa intesa o su richiesta della Autorità di Pubblica Sicurezza e degli Organi di Polizia, dispone l'utilizzo del sistema di video-sorveglianza in dotazione alla Polizia Locale, compresi i sistemi di lettura targhe e ZTL, ai fini di prevenzione e repressione di atti delittuosi anche nell'ambito del più ampio concetto di "sicurezza urbana", così individuata secondo il Decreto Ministro Interno 5 agosto 2008 decreto legge 20 febbraio 2017, n. 14 recante "Disposizioni urgenti in materia di sicurezza delle città" convertito con legge n. 48/2017.

Tutto il sistema di video-sorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata. L'attività di video-sorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità succitate, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.

L'uso dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate alla normativa vigente in materia di "privacy" con un'apposita regolamentazione

Quali sono le risorse di supporto ai dati?

Sistema di videosorveglianza urbana: le immagini vengono gestite da un Software dedicato

Sistema di lettura targhe: le immagini vengono gestite e salvate su un server collegato ad internet.

Fototrappole: le immagini vengono salvate a bordo della fototrappola, sfruttando innovative tecnologie di analisi video e intelligenza artificiale integrate con componenti hardware di altissima qualità raggiungibili da remoto (router 4G a bordo).

Valutazione: Accettabile

PRINCIPI FONDAMENTALI

Proporzionalità e necessità

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza ambientale risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose in quanto non risulta possibile, e laddove messo in atto è risultato non efficace, il ricorso a strumenti e sistemi di controllo alternativi.
La liceità è data dall'art. 6 par. 1 del GDPR, in quanto "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".
Il trattamento avviene altresì a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, ai sensi dell'art. 1 comma 2 del Dlgs 18 maggio 2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio". Il Comune di Ferentino, attraverso il Comando di Polizia Locale, effettua il trattamento di dati personali mediante impianti di videosorveglianza urbana, sia di osservazione che di contesto, ed altri sistemi di ripresa immagini di dati personali quali telecamere per lettura targhe, foto-trappole e Autoscan; possono altresì essere previsti altri sistemi di videosorveglianza come specificato di seguito. In particolare, l'uso di tutti i sistemi e tipologie di videosorveglianza del territorio comunale è finalizzato a:
a) tutelare la sicurezza urbana di cui alla L. n. 38/2009 ss.mm.ii, Decreto del Ministro dell'Interno del 05 agosto 2008 e decreto legge 20 febbraio 2017, n. 14 nonché secondo le modalità previste dal capitolo n. 5.1 del Provvedimento del Garante Privacy in materia di video-sorveglianza dd. 08/04/2010;
b) prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale secondo le modalità previste dal capitolo n. 5.1 del Provvedimento del Garante Privacy in materia di video-sorveglianza dd. 08/04/2010;
c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale ed a prevenire eventuali atti di vandalismo o danneggiamento;
d) controllare determinate aree e/o specifici siti comunali potenzialmente esposti a rischi di vandalismo o danneggiamento quali, a mero titolo esemplificativo, parchi, impianti sportivi e strutture ludico-ricreative;
e) al monitoraggio del traffico veicolare, al fine di prevenire o gestire problematiche inerenti la viabilità;
f) a tutelare in particolare coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un adeguato grado di sicurezza nelle zone anche per le finalità previste dal "Decreto sicurezza" approvato con Decreto Legge 23 febbraio 2009, n. 11 e convertito nella legge 23 aprile 2009, n. 38;
g) controllare ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose nonché per monitorare il rispetto delle disposizioni concernenti modalità, tipologia dei rifiuti scaricati ed orario di deposito dei rifiuti, la cui violazione può essere sanzionata amministrativamente (art. 13, legge 24 novembre 1981, n. 689), secondo le previsioni di cui al capitolo n. 5.2 del Provvedimento del Garante Privacy in materia di video-sorveglianza dd. 08/04/2010. Attualmente, con l'entrata in vigore della legge 137/2023 l'abbandono dei rifiuti compiuto da *chiunque* comporta l'applicazione di una ammenda penale e pertanto si rinvia a quanto sopra indicato in tema di prevenzione dei reati;

h) prevenire eventuali atti di vandalismo e/o danneggiamento ovvero spaccio di sostanze stupefacenti presso Istituti scolastici in casi di stretta indispensabilità ed attivando gli impianti interni esclusivamente negli orari di chiusura degli Istituti secondo le modalità previste dal capitolo n. 4.3 del Provvedimento del Garante 4 Privacy in materia di video-sorveglianza dd. 08/04/2010.
i) rilevare violazioni al Codice della strada mediante l'uso di sistemi OCR (Optical Character Recognition) per riconoscimento delle targhe veicolari;
l) tutelare l'ordine e la sicurezza pubblica e prevenire, accertare e reprimere i reati mediante il controllo dei veicoli in transito; le informazioni delle targhe inserite in "liste di controllo" particolari potranno essere condivise con le altre Forze dell'Ordine a seguito di specifico "Protocollo operativo" predisposto e sottoscritto dal Comitato provinciale per l'ordine e la sicurezza pubblica;
m) supportare operazioni di protezione civile.

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Sulla base di quanto sopra indicato la liceità del trattamento è individuabile ex art. 6 par. 1 lett. E del GDPR, art. 5 del Dlgs 18 maggio 2018, n. 51 e art. 23, comma 1, del d.P.R. n. 15 del 2018.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati vengono raccolti solo per l'attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale e per la ricostruzione, in tempo reale, della dinamica di atti vandalici o fatti criminosi o azioni di teppismo nei luoghi pubblici di principale frequentazione, anche a tutela del patrimonio pubblico.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Le basi giuridiche del trattamento sono le lettere c) ed e) dell'art. 6 del Reg. (UE) 2016/679: "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" e "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".

Valutazione: Accettabile

I dati sono esatti e aggiornati?

Di norma i dati sono acquisiti avuto riguardo al "tempus commissionis" solo nel caso venga rilevata una condotta illecita ovvero acquisiti sulla scorta dei relativi aggiornamenti delle banche dati consultate.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Per i dati trattati per finalità di controllo, monitoraggio e valutazione traffico veicolare la conservazione dei dati per il tempo di legge (5 anni ed oltre in caso di riscossione coattiva) è necessaria per poter agire legittimamente per la riscossione delle sanzioni; al termine del periodo di conservazione i documenti sono cancellati in modo irreversibile.

Nel momento in cui se ne presenti l'esigenza a fronte constatazione di fatto illecito un addetto autorizzato al trattamento visiona i firmati registrati.

Il fascicolo viene consegnato con modalità sicure al soggetto che avvia e svolge il procedimento amministrativo.

Per tutte le altre finalità il termine massimo di durata della conservazione dei dati è limitato "*ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione*" ai sensi del paragrafo 3.4.3 del provvedimento 08.04.2010 Garante Privacy. In relazione alle capacità di immagazzinamento dei dati forniti sui server, in condizioni di normale funzionamento le immagini riprese in tempo reale si sovrascrivono a quelle registrate, in piena osservanza della normativa vigente sulla privacy.

Valutazione: Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

In ottemperanza al decreto legislativo 10/08/2018, n. 101 nelle zone in cui sono posizionate le telecamere è affissa adeguata segnaletica con cartelli conformi alle indicazioni dell'Autorità Garante. Si specifica inoltre che nella sezione "privacy" del sito web istituzionale del Comune viene riportata l'informativa completa sul trattamento dei dati di videosorveglianza ai sensi dell'art. 13 del reg. 679/16.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Non è richiesto il consenso degli interessati, le basi giuridiche del trattamento sono le lettere c) ed e) dell'art. 6 del Reg. (UE) 2016/679: "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" e "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

In relazione al trattamento dei dati personali, è assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificarne le finalità, le modalità del trattamento e di ottenerne l'interruzione nel caso di utilizzo illecito, in particolare per la carenza dell'adozione delle idonee misure di sicurezza o per l'uso indebito da parte di soggetti non autorizzati. I diritti di cui al presente articolo riferiti a dati personali concernenti persone decedute, possono essere esercitati dagli eredi, da chi abbia un interesse proprio, da chi agisca a tutela dell'interessato o per ragioni familiari considerate particolarmente meritevoli di protezione. Nel caso di esito negativo alle istanze di cui al presente articolo, l'interessato può

rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Ai sensi dell'art. 15 del Regolamento (UE) relativo al diritto di accesso dell'interessato:

1. l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento;
3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi; se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune;
4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.
In ragione alla tipologia di trattamento che riguarda filmati l'interessato e di quanto disposto al punto 4 dell'art. 15 del Reg. (UE) 2016/679 l'interessato non può avere accesso ai filmati in forma integrale perché potrebbero contenere immagino di altri soggetti così violando i diritti e le libertà altrui. Ne consegue che in caso di esercizio del diritto di accesso con riferimento al punto 3 dell'articolo 15 dell'RGPD il titolare prima di fornire copia di quanto richiesto dovrà verificare che non siano presenti immagini relative ad altre persone e nel caso ne riscontri la presenza provvedere all'oscuramento delle immagini relative alle persone diverse dall'interessato.
Per l'esercizio del diritto di accesso, l'interessato deve presentare istanza per l'esercizio dei diritti dell'interessato al Responsabile della Protezione dei dati del Comune, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sul sito istituzionale del Comune nella sezione "Privacy") ovvero al Designato o direttamente al Titolare.
Non è possibile per l'interessato esercitare il diritto alla portabilità ai sensi dell'art. 20 del Reg. (UE) 2016/679 in quanto è un trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento e come tale escluso dalla possibilità di esercizio di tale diritto dal punto 3 dello stesso articolo.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Ai sensi dell'art. 16 GDPR l'interessato ha il diritto di ottenere la rettifica di dati personali inesatti ovvero l'integrazione di dati personali incompleti.
Considerati i tempi ristretti di conservazione dei dati e la tipologia di trattamento potrebbe essere impossibile procedere con l'esercizio di tali diritti.
Nel caso si verificano le condizioni per l'esercizio del diritto di rettifica, l'interessato deve presentare istanza per l'esercizio dei diritti dell'interessato al Responsabile della Protezione dei dati del Comune, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sul sito istituzionale del Comune nella sezione "Privacy") ovvero al Designato o direttamente al Titolare.
Ai sensi dell'art. 17 RGDP l'interessato ha il diritto alla cancellazione dei suoi dati: 1) nel caso che non siano più necessari rispetto alle finalità di raccolta; 2) nel caso si opponga al trattamento e non vi siano altri motivi legittimi per procedere con lo stesso; 3) nel caso i dati siano trattati illecitamente da parte del titolare del trattamento; 4) nel caso i dati debbano essere cancellati per adempiere ad un obbligo di legge cui è soggetto il titolare del trattamento. In tutti questi casi il titolare del trattamento dovrà procedere alla cancellazione di tali dati senza ingiustificato ritardo.

Non si applica il diritto alla cancellazione quando vi è un obbligo di legge da rispettare e/o un compito da svolgere nel pubblico interesse ovvero l'esercizio di pubblici poteri cui è investito il titolare del trattamento e non si applica per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria (art. 24 Cost.).

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Ai sensi dell'art. 18 GDPR l'interessato ha il diritto di ottenere la limitazione del trattamento dei dati personali che lo riguardano quando: 1) contesta l'esattezza dei dati personali (nei limiti della durata di conservazione); 2) il trattamento è illecito; 3) l'interessato ha necessità di utilizzare i suoi dati per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria benché il titolare non abbia più bisogno di questi dati; infine, quando l'interessato si oppone al trattamento dei suoi dati.

Nel caso si verificano le condizioni per l'esercizio del diritto di limitazione, l'interessato deve presentare istanza per l'esercizio dei diritti dell'interessato al Responsabile della Protezione dei dati del Comune, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sul sito istituzionale del Comune nella sezione "Privacy") ovvero al Designato o direttamente al Titolare.
Ai sensi dell'art. 21 GDPR l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettera e), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento deve astenersi dal trattare ulteriormente i dati personali salvo sia in grado di dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Nel caso si verificano le condizioni per l'esercizio del diritto di opposizione, l'interessato deve presentare istanza per l'esercizio dei diritti dell'interessato al Responsabile della Protezione dei dati del Comune, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sul sito istituzionale del Comune nella sezione "Privacy") ovvero al Designato o direttamente al Titolare.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi dei responsabili del trattamento sono definiti dal Regolamento per la disciplina della videosorveglianza nel territorio comunale di Ferentino approvato con delibera del Consiglio Comunale n. 38 del 26.09.2023.

Valutazione: accettabile

Nello specifico devono essere nominati Responsabili del trattamento:

- la ditta che effettua la manutenzione dei dispositivi elettronici;
- la ditta che effettua la manutenzione del software;
- tutti i soggetti esterni che svolgono operazioni relative al trattamento dei dati ai fini manutentivi.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non sono trasferiti al di fuori dell'Unione Europea.

Valutazione: Accettabile

RISCHI E MISURE

Misure esistenti o pianificate

Crittografia

Il software contiene dati criptati (sia per il sistema di videosorveglianza fissa sia per quello mobile). Per cui in caso di sottrazione delle immagini non si correrebbe alcun rischio in quanto le immagini sono soggette a crittografazione.

Valutazione: Accettabile

Controllo degli accessi logici

L'accesso e controllato da password di lunghezza minima di 8 caratteri composta da lettere, numeri e caratteri speciali.

Valutazione: Accettabile

Tracciabilità

Sono adottati appositi registri che documentano le operazioni di visualizzazione delle immagini, le operazioni di scarico delle immagini relative a fatti illeciti.

Valutazione: Accettabile

Archiviazione

Ordinari sistemi di sicurezza. Archiviazione in Cloud

Valutazione: Accettabile

Minimizzazione dei dati

Il numero di persone identificate è ridotto in conseguenza al fatto che l'accesso alla visione delle immagini è limitato alle sole persone autorizzate formalmente al trattamento e in considerazione del fatto che essendo immagini è necessario procedere all'eventuale identificazione della persona e l'identificazione avviene solo nel caso sia rilevato un fatto illecito, i dati sono conservati per un periodo limitato.

Valutazione: Accettabile

Gestione postazioni

L'accesso alle immagini è limitato alle sole persone autorizzate formalmente al trattamento.
Per accedere alle postazioni è necessario essere fisicamente presenti all'interno degli uffici della Polizia Locale e l'accesso alle postazioni è protetto da login e password.

Valutazione: Accettabile

Sicurezza dei documenti cartacei

Conservazione in archivi non accessibili al pubblico

Valutazione: Accettabile

Vulnerabilità

Antivirus. Archiviazione in Cloud

Valutazione: Accettabile

Lotta contro il malware

Sistemi di sicurezza antivirus e di protezione di rete (intranet; firewall, ecc.)

Valutazione: Accettabile

Backup

Periodici e in cloud

Valutazione: Accettabile

Manutenzione

In ambiente dedicato. Il sistema è affidato in manutenzione che è effettuata o recandosi sul posto o attraverso l'accesso al server dall'esterno attraverso sw di accesso remoto che viene attivato dal personale interno solo per il periodo necessario.

Valutazione: Accettabile

Sicurezza dei canali informatici

Rete intranet dell'ente. Firewall

Valutazione: Accettabile

Controllo degli accessi fisici

La postazione per la visualizzazione delle immagini è collocata all'interno del comando di Polizia Locale, in postazioni non accessibili all'utenza e/o soggetti esterni; la stanza è chiusa e l'accesso all'ufficio è gestita dal Comandante dell'ufficio di Polizia Locale.

Valutazione: Accettabile

Sicurezza dell'hardware

I server sono ubicati in locali dedicati. I PC sono accessibili mediante password

Valutazione: Accettabile

Prevenzione delle fonti di rischio

Misure sia fisiche, logiche e organizzative.

I soggetti "autorizzati" a trattare i dati di videosorveglianza sono nominati con specifici atti, come da Regolamento Comunale, e sono istruiti e formati sul corretto trattamento.
Per l'accesso al Comando di persone non dipendenti è permesso solo dopo l'identificazione e sono accolte da un dipendente del servizio cui accede.
Molte delle funzionalità di controllo degli accessi possono essere abilitate o disabilitate dai clienti in base alle esigenze o possono essere modificate per soddisfare un livello specifico di rischio. Le impostazioni predefinite per queste funzionalità di sicurezza sono state scelte per fornire un forte livello di sicurezza, pur mantenendo flessibilità e praticità.

In merito alle autorizzazioni:
Gestione granulare delle autorizzazioni basata sui ruoli.
Gestione delle autorizzazioni dell'applicazione (ad esempio, consentire a utenti specifici di utilizzare l'interfaccia basata sul Web).
Integrazione con i servizi directory per una gestione degli utenti semplificata e sicura.

In merito al controllo e reporting e di gestione degli utenti:
Registrazione dettagliata delle attività dell'amministratore e dell'utente a prova di manomissione.
Portale Web di amministrazione intuitivo per gestire utenti, autorizzazioni e ruoli.

In merito alla condivisione di dati:
Condivisione di prove all'interno dell'agenzia, tra agenzie ed esterne senza trasferimento di dati, duplicazione dei dati, supporti fisici o allegati e-mail.
Registrazione dettagliata della catena di custodia durante la condivisione.
Revocare l'accesso al contenuto condiviso in precedenza.

Impedire a un destinatario di contenuto condiviso di scaricare o ricondividere le prove.

Valutazione: Accettabile

Gestione del personale

Gli addetti al trattamento sono limitati nel numero, istruiti, aggiornati e responsabilizzati.

Valutazione: Accettabile

Gestione delle politiche di tutela della privacy
L'ufficio di Polizia locale ha implementato una politica tesa a garantire l'adeguatezza della protezione dei dati personali nominando e istruendo i soggetti interni autorizzati ad effettuare il trattamento dei dati personali e nominando responsabili esterni al trattamento esclusivamente soggetti esterni che effettuano trattamenti per conto dell'ufficio di Polizia locale in grado di fornire adeguate garanzie di affidabilità.
Il titolare al momento dispone di un impianto documentale relativo alle misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.

Valutazione: Accettabile

Gestione dei terzi che accedono ai dati

Gestione in outsourcing con soggetti muniti di adeguate credenziali e di idonee misure di sicurezza in materia di tutela della riservatezza.

Valutazione: accettabile

Piano d'azione / misure correttive:

Tali soggetti devono essere nominati Responsabili del trattamento ai sensi dell'art. 28 GDPR.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali
È stata approvata una procedura e un'organizzazione operativa per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati.

Valutazione: Accettabile

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure applicate/pianificate?

Si ritiene il livello di rischio **Basso**.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Si ritiene la circostanza **Improbabile**

Rischi Accesso

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Sistema di videosorveglianza urbana: in caso di sottrazione delle immagini non si correrebbe alcun rischio in quanto le immagini sono soggette a crittografazione.

Sistema di lettura targhe: in caso di sottrazione delle immagini non si correrebbe alcun rischio in quanto le immagini sono soggette a crittografazione

Fototrappole: in caso di sottrazione non si correrebbe alcun rischio in quanto le immagini sono soggette a crittografazione

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso abusivo al server o accesso abusivo presso il Comando.

Accesso illegittimo ai luoghi di lavoro, malware, hacker, cancellazione involontaria, distruzione del dispositivo, furto del dispositivo, cancellazione volontaria

Sistema di videosorveglianza urbana: il sistema non è connesso ad internet quindi non ci possono essere vulnerabilità "logiche" ma esclusivamente fisiche dovute all'ingresso presso il Comando, all'ingresso presso la Sala Macchine o presso un armadietto stradale.

Quali sono le fonti di rischio?

Fonte umana esterna, Fonte non umana, Fonte umana interna

Accesso tramite internet o accesso abusivo fisicamente in Comando.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Gestione postazioni, Sicurezza dei documenti cartacei, Backup, Vulnerabilità, Lotta contro il malware, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Gestione del personale, Gestione delle politiche di tutela della privacy, Gestione dei terzi che accedono ai dati, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Basso

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

La stima individua l'evento come **Improbabile.**

Valutazione: **Accettabile**

Rischi Modifica

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Conoscenza da parte di terzi del fatto che è stata posta in essere una condotta costituente illecito amministrativo, Cancellazione parziale dati, individuazione errata destinatari provvedimenti, non attribuzione di un illecito commesso

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accesso illegittimo ai luoghi di lavoro, hacker, malware, furto del dispositivo

Quali sono le fonti di rischio?

Fonte umana esterna, Fonte umana interna, Fonte non umana

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Gestione postazioni, Sicurezza dei documenti cartacei, Backup, Vulnerabilità, Lotta contro il malware, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Gestione del personale, Gestione delle politiche di tutela della privacy, Gestione dei terzi che accedono ai dati, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile.

Valutazione: Accettabile

Rischi Perdita

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Cancellazione dati, Non attribuzione di un illecito commesso

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Accesso illegittimo ai luoghi di lavoro, Furto del dispositivo, distruzione del dispositivo, cancellazione involontaria, hacker, malware

Quali sono le fonti di rischio?

Fonte non umana, Fonte umana esterna, Fonte umana interna

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Gestione postazioni, Sicurezza dei documenti cartacei, Backup, Vulnerabilità, Lotta contro il malware, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Gestione del personale, Gestione delle politiche di tutela della privacy, Gestione dei terzi che accedono ai dati, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Il rischio è minimo in dipendenza del fatto che hardware e software sono riservati ed isolati e non accessibili all'utenza

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, Hardware e software sono riservati ed isolati e non accessibili all'utenza

Valutazione: Accettabile

Tabella Rischi

Panoramica dei rischi

Panoramica

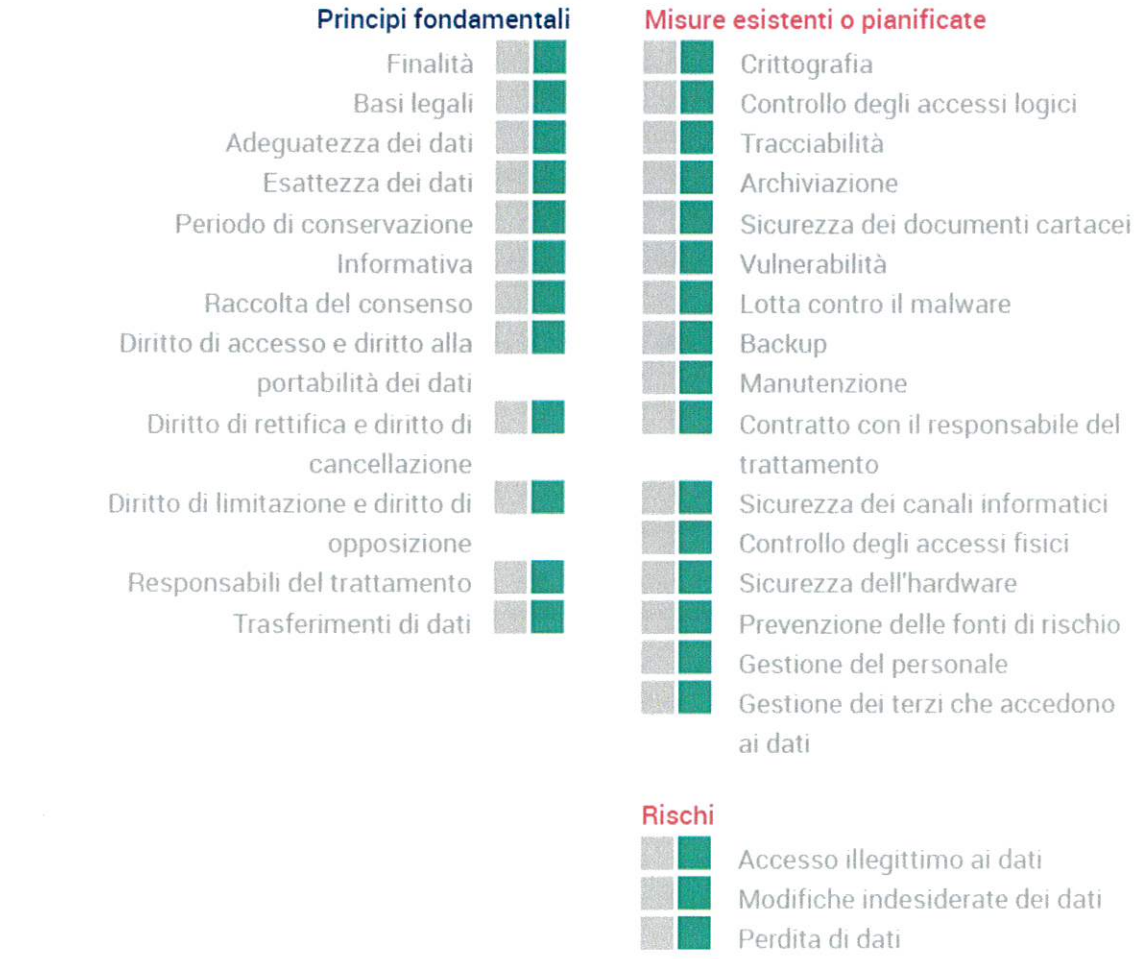
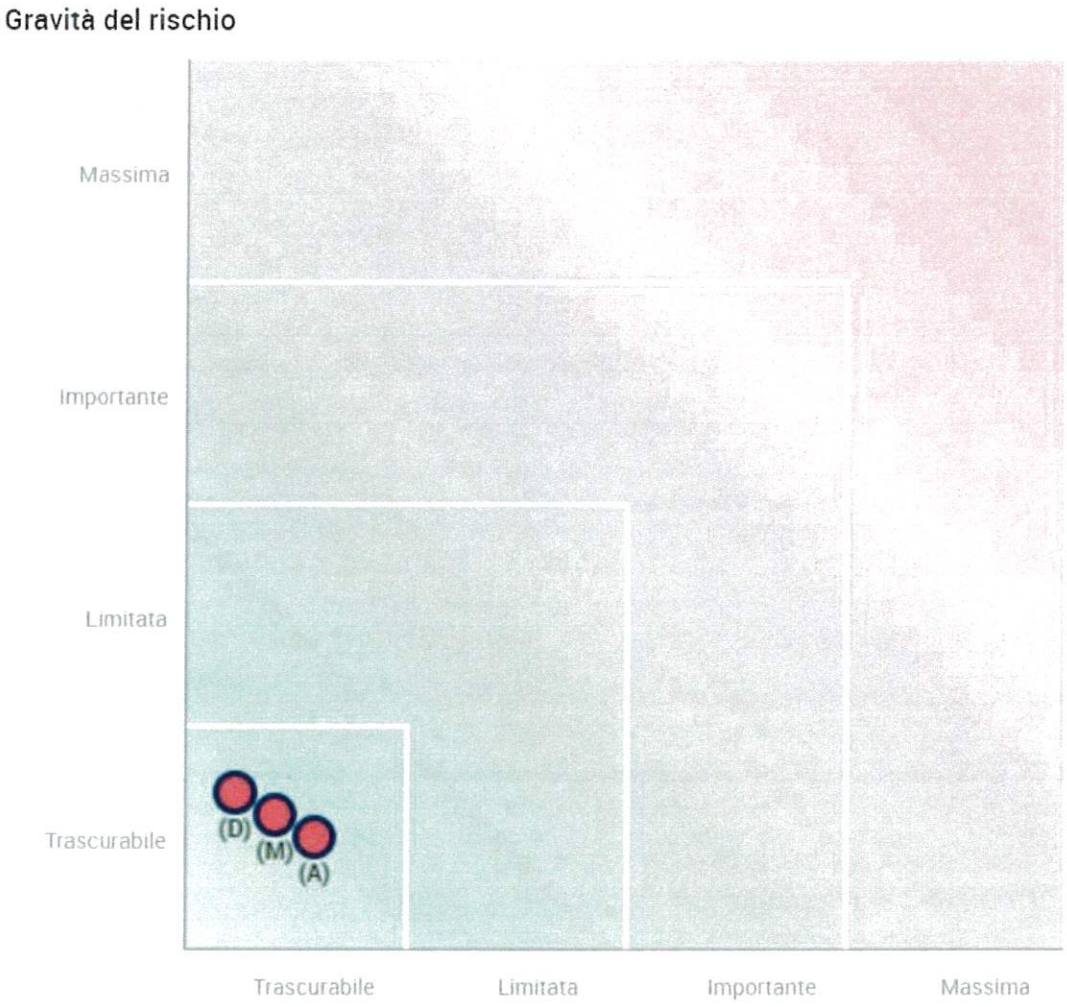
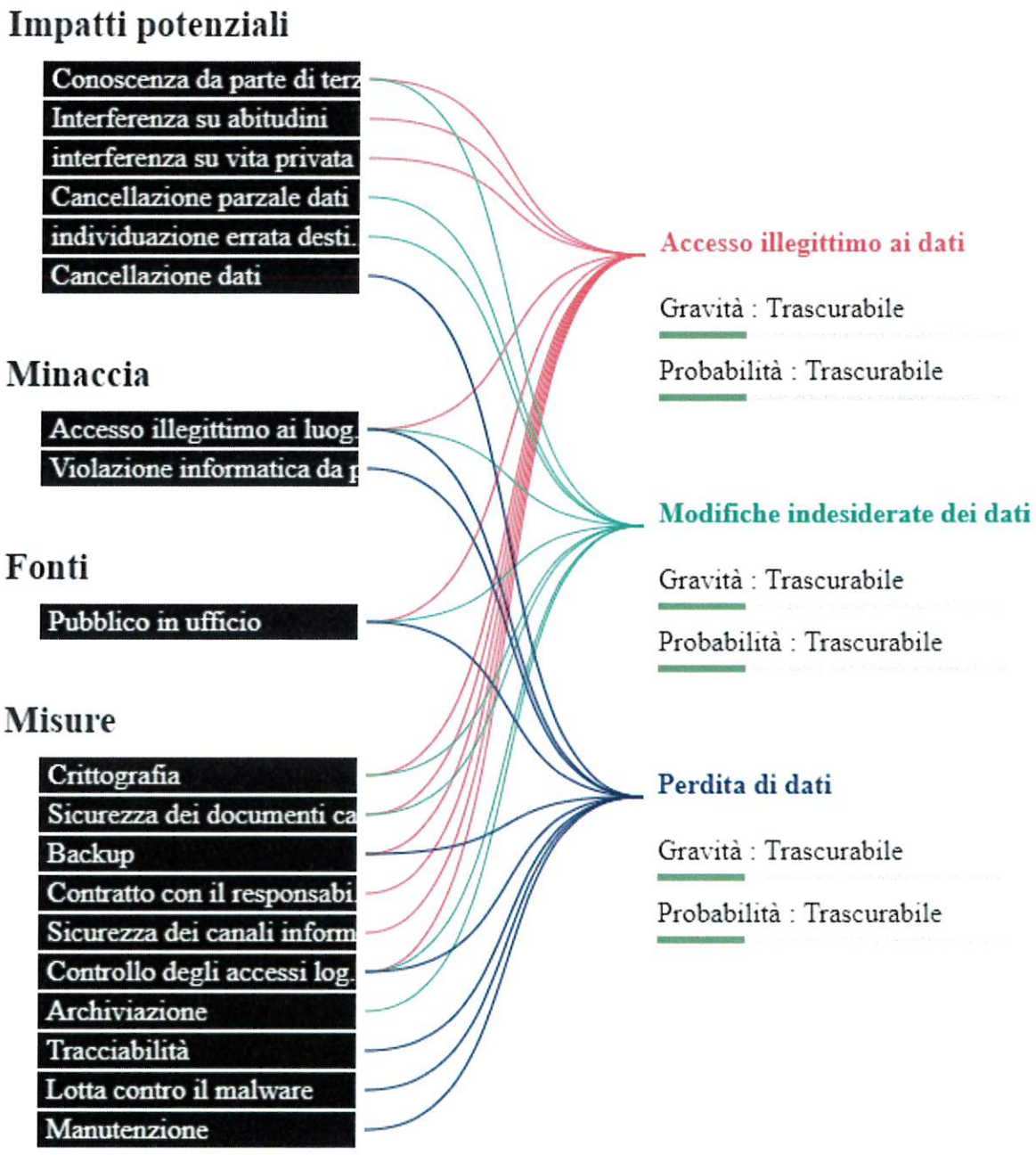


Tabella Gravità del Rischio



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Tabella Impatti, Minacce, Fonti, Misure



PARERE DEL DPO/RPD:

"In seguito ad attenta analisi del presente documento, visto l'art. 39 par. 1 lett. C del Reg. 679/2016, il DPO ritiene che i rischi per i diritti e le libertà degli interessati soggetti alle riprese, a seguito dell'adozione delle misure di mitigazione del rischio indicate dall'ente, possano essere qualificati come rischi accettabili in relazione alle finalità perseguite dal trattamento in oggetto. Il sistema nel suo complesso coniuga in un ragionevole equilibrio il diritto alla riservatezza e protezione dei dati personali dei cittadini con le attività di sicurezza urbana e tutela, prevenzione e gestione delle criticità di ordine pubblico in capo alle forze di Polizia Locale, come da competenza normativa. Nello specifico, come dai colloqui e decisioni intercorse, non sono mai state attivate funzionalità speciali di controllo "intelligente" del Sistema di videosorveglianza né di identificazione anche biometrica degli interessati, in ossequio alla presente valutazione di impatto, alle indicazioni dell'Autorità Garante per la protezione dei dati personali ed alle novità in materia dettate dal Decreto Legge 8 ottobre 2021, n. 139. Pertanto nel complesso, alla data odierna, non si ritiene esistente un "rischio elevato" come inteso dall'art. 35 GDPR; per tale ragione, inoltre, non si rende necessario procedere con la Consultazione preventiva ex art. 36 GDPR."

Ferentino, 04/01/2024

Il Responsabile

dott. Piergianni Fiorletta

COMUNE DI FERENTINO

Il DPO

Dott. Massimo Genovesi