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 soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati. Per questo motivo, i criteri

[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

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 il sistema di "fototrappole"comunale ai fini di fronteggiare l'abbandono di rifiuti e/o l'utilizzo scorretto da parte dei cittadini delle c.d. eco-piazzole trattandosi di un sistema di videosorveglianza dedicato che può realizzare una *"sorveglianza sistematica su larga scala di una zona accessibile al pubblico" e in quanto tale possa definirsi un trattamento che "possa presentare rischi elevati ai sensi dell'articolo 35, paragrafo 3, del Regolamento (UE) 2016/679.*

Il Garante per la Protezione dei Dati Personali con l Provvedimento generale 8 aprile 2010 in tema di videosorveglianza al **punto 5.2** si occupa dell'utilizzo di un sistema di videosorveglianza finalizzato al monitoraggio delle aree adibite a "deposito dei rifiuti".

In particolare, il provvedimento distingue a seconda che l'impianto di videosorveglianza sia utilizzato per:

1. controllare l'utilizzo abusivo di aree impiegate come discariche di materiali e sostanze pericolose;
2. controllare il rispetto delle disposizioni (esempio ordinanze comunali) concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente ai sensi dell'art. 13, legge 24 novembre 1981, n. 689).

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 fototrappole, siano rilevabili "almeno due di questi criteri" potendosi compiere con tali dispositivi:

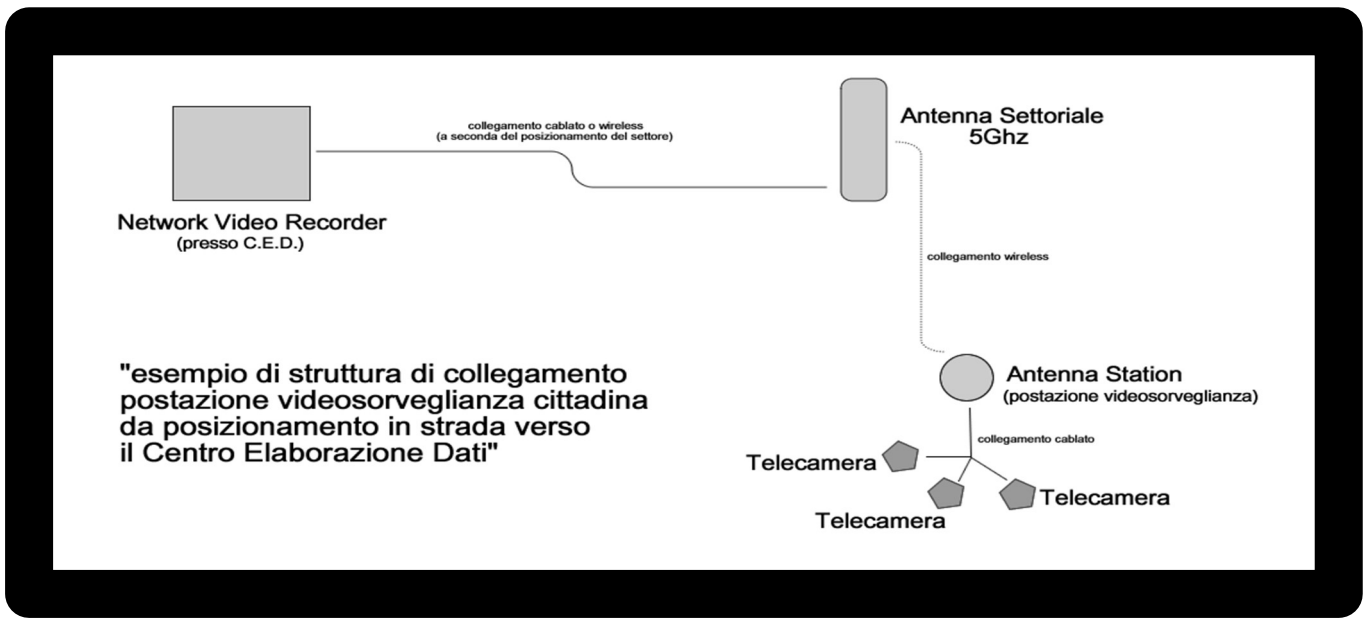
1. un processo decisionale automatizzato;
2. un monitoraggio sistematico;
3. di dati sensibili o dati aventi carattere altamente personale;
4. su larga scala;
5. che possono comprendere anche dati relativi a interessati vulnerabili;
6. e che potrebbero comprendere utilizzi innovativi o applicazione di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

Schema del sistema

Telecamere		Tipologia	Risoluzione	Compressione	Protocollo	Compatibilità	Adds			Backup
Axis	215 PTZ	Dome	704*576	4CIF	HTTP / HTTPS	ONVIF	audio input	non attivo		NVR
Planet	ICA-3150	Bullet	1280*720	H.264	RTSP /HTTPS	ONVIF	---	---	---	NVR
	ICA-3250	Bullet	1280*720	H.264	RTSP /HTTPS	ONVIF	audio input	non attivo	---	NVR
	ICA-4150	Dome	1280*720	H.264	RTSP /HTTPS	ONVIF	---	---	---	NVR
Hikvision	DS-2CD1023G0E-I	Bullet	1920*1080	H.265	RTSP /HTTPS	ONVIF	---	---	---	NVR
	DS-2CD2020F-I	Bullet	1920*1080	H.265	RTSP /HTTPS	ONVIF	---	---	---	NVR
	DS-2CD2625FWD-IZS	Bullet	1920*1080	H.265	RTSP /HTTPS	ONVIF	SD Card	cifratura	Face Detect	NVR
	DS-"DF5284-A	Dome	1920*1080	H.265	RTSP /HTTPS	ONVIF	---	---	---	NVR
	DS-2CD4A26FWD-IZS/P	Bullet	1920*1080	H.265	RTSP /HTTPS	ONVIF	SD Card	cifratura	Lettura Targhe	NVR
	iDS-TCM203-A	Bullet	1920*1079	H.265	RTSP /HTTPS	ONVIF	SD Card	cifratura	Lettura Targhe	NVR
	iDS-2CD7A46G0-IZHS	Bullet	1920*1080	H.265	RTSP /HTTPS	ONVIF	SD Card	cifratura	Face Detect	NVR
MINI DV	V4 Camera	MicroCam	1920*1080	H.264	HTTP / HTTPS	ONVIF	SD Card	NO cifratura	Fototrappola	Locale su SD
"No Brand"	SpyCam	Finto Vaso	1920*1080	H.264	HTTP / HTTPS	ONVIF	SD Card	NO cifratura	Fototrappola	Locale su SD
"No Brand"	SpyCam	Finta Roccia	1920*1080	H.264	HTTP / HTTPS	ONVIF	SD Card	NO cifratura	Fototrappola	Locale su SD
Marviosafer	Starlight Mini PTZ	Finto Contatore	1920*1080	H.264	HTTP / HTTPS	ONVIF	SD Card	NO cifratura	Fototrappola	Locale su SD

Network Video Recorder		Tipologia	Canali	Compressione	Protocollo	Compatibilità	Adds			Backup
Hikvision	DS-7616NI-K2	RackMount	16	H.264	RTSP /HTTPS	ONVIF	---	Cifratura	---	HDD (RAID1)
	DS-9632NI-I8	RackMount	32	H.264	RTSP / HTTPS	ONVIF	---	Cifratura	---	HDD (RAID1)
	DS-9664NI-I8	RackMount	64	H.264	RTSP / HTTPS	ONVIF	---	Cifratura	---	HDD (RAID1)

Antenne (CPE)		Tipologia	Frequenza	Descrizione	Posizionamenti presso
Mikrotik	RB433AH	Settore	5GHz	Antenna settoriale aggregazione collegamenti	Sedi Comunali di Via del Plebiscito e di Piazza VI Dicembre, Palazzo Tiravanti, Prefettura, Liceo Classico, Liceo Magistrale, Stadio Benito Stirpe, Corso Lazio, Primaria Via Verdi
	RB911G	Settore	5GHz	Antenna settoriale aggregazione collegamenti	
	RB921GS	Settore	5GHz	Antenna settoriale aggregazione collegamenti	
	RB941	Station	5GHz	Antenna di collegamento postazione	su ogni postazione stradale
	RBSXT5N	Station	5GHz	Antenna di collegamento postazione	
	RBSXTSQ5N	Station	5GHz	Antenna di collegamento postazione	



Installazioni eseguite:	
Settori:	22
Antennte Station:	133
Telecamere:	531
Fototrappole:	40
NVR:	43

Note:
Si precisa che le "fototrappole" non sono posizionate nella totalità dei pezzi disponibili ma vengono installate secondo il piano predisposto dal Settore Ambiente e dalla Polizia Locale.

Di seguito si riportano tutte le installazioni eseguite sul territorio comunale:

Indirizzo	Dettaglio	CPE	TLC
Piazzale Vivoli	Piazzale + Via Coroni	1	2
Via Aldo Moro	Incroci vs Via Po, Via Isonzo, Via Tagliamento, Via del Casone, Piazzale De Matthaeis	7	12
Via Puccini	compreso Sottopasso	2	5
Incrocio Marchegiani	vs Via Albinoni, vs Via Palestrina	1	3
Largo Toscanini	vs Via Marittima, vs Via Fontana Unica, vs Via Don Minzoni	1	3
Via Fosse Ardeatine	nei pressi Scuola Ricciotti	1	3
Zona Fontanelle	vs Via Ciamarra, vs Via Mola Vecchia, vs Via Rosselli, vs Viale Mazzini	2	6
Zona Parco Matusa	Rotatoria, vs Via Aldo Moro, vs Viale Mazzini, vs Via Piave, vs Via Marittima	1	5
Via Marittima	Incrocio vs viale Europa, vs Via Ciamarra	1	4
Via Ciamarra	vs Via Fontana Unica, vs Fontanelle	1	2
Viadotto Biondi	entrambi i sensi di marcia	1	2
Piazza della Libertà	Piazza + Via del Plebiscito	1	3
Incrocio Sant'Antonio	vs Via del Cipresso, vs Viale Napoli, vs Via Acciaccarelli, vs Corso della Repubblica, Piazza IV Novembre	1	6
Zona San Liberatore	vs Via Impradessa	1	3
Largo Amendola	vs Largo Turriziani, vs Viale Mazzini	1	3
Corso Lazio	vs Via Rieti, vs Via Palestrina, vs Sottopasso	3	7
Via Minghetti	entrambe le direzioni	0	2
Via Montecassino	Zona parcheggio Provincia	2	5
Via Piave	Rotatoria + vs le varie direzioni	1	6
Via Mascagni	Rotatoria + vs le varie direzioni	1	5
Piazza Vittorio Veneto	Piazza + vs Corso della Repubblica	0	6
Via Sacra Famiglia	Piazza + Giardinetti	2	4
Piazzale Kambo	Zona Stazione Ferroviaria	2	5
Zona Stadio Benito Stirpe	Rotatorie varie + le varie direzioni	1	16
Via Michelangelo	Zona Conservatorio	2	4
Piazza Garibaldi	Piazza + vs Via Minghetti, vs A.Paleario	2	5
Via Nuova	vs Via Aldo Moro	1	3
Corso della Repubblica	zona Le Terrazze	1	2

Piazza Gramsci	Piazza + vs Via Marconi, vs A.Latina	1	3
Corso della Repubblica	Zona Biblioteca Comunale	1	8
Via De Gasperi	Zona Piloni	0	2
Via Maria	Intero tratto + vs Via Caio Mario	2	4
Via Cinque Vie	Zona aeroporto	1	2
Via Madonna delle Rose	Incrocio vs Via Selvotta, vs Via Selva Casarino, Via Fermi	3	8
Via Monti Lepini	Zona incrocio Via Conti, zona uscita Autostrada	3	8
Piazza VI Dicembre	Zona Sede Comunale	0	7
Via Prefelci	vs Via Brighindi, vs Via Cerceto	1	2
Via Pignatelle	Incrocio vs Via Melocce	2	5
Via Casilina Nord	Incrocio Via La Torre	1	2
Via Cervona	Incrocio vs Frosinone	1	2
Via Vetiche	Incrocio vs Torrice, vs Frosinone	1	2
Via Colle Vecchino	Incrocio vs Santissima, vs Maniano	1	2
Via Colle Timio	Incrocio	1	1
Via Le Rase	vs Cavalcavia	2	3
Via Landolfi	Incrovio vs Via Armando Fabi, vs Via Monti Lepini	1	2
Via Forcella	entrambe le direzioni	1	2
Via San Gerardo	vs Tunnel	1	1
		65	**198**

Di seguito si riportano tutte le installazioni eseguite presso sedi ed istituti:

Sede - Istituto	Indirizzo	CPE	TLC	NVR
Infanzia Collecannuccio	Via Collecannuccio	2	4	1
Liceo Turriziani	Via Acciaccarelli	5	2	2
Parco Matusa	Viale Mazzini	1	9	1
Palazzo Comunale	Via del Plebiscito	2	32	1
Ascensore Inclinato	Via Veccia	1	20	1
Sede Comunale Centro	Piazza VI Dicembre	2	4	6
Sede MTC	Via Armando Fabi	0	4	12
Museo Archeologico	Via XX Settembre	0	7	1
Polivalente	Viale Mazzini	1	3	0
Sede Forum (Polizia Locale)	Piazzale Europa + zona Selva Piana	7	15	1
Infanzia Fantasiia	Via Fedele Calvosa	1	3	0
Villa Comunale	Via Marco Tullio Cicerone	5	32	1
Cimitero	Via De Carolis	10	32	2
Centro Sociale Integrato Disabili	Via Sodine	0	6	1
Casa della Cultura (Ex Mattatoio)	Viale Roma	0	5	1
Secondaria Aldo Moro	Via Mastruccia	1	16	1
Centro Sociale Corso lazio	Corso Lazio	1	4	1
Primaria De Luca	Viale America Latina	0	2	0
Centro Sociale Anziani Via Adige	Via Adige	0	2	0
Centro Sociale Anziani Messia	Via Portogallo	0	10	1
Infanzia Madonna della Neve	Via Barbagallo	0	3	0
Centro Sociale Anziani Fiordaliso	Corso della Repubblica	1	1	0
Primaria De Matthaeis	Via De Matthaeis	0	1	0
CPA Lombardo Radice	Via Mascagni	0	13	1
Infanzia Spinelli	Via Gaeta + Zona Fornaci	2	6	0
Primaria Giovanni XXIII	Via Albinoni	0	4	0
Primaria Via Verdi	Via Verdi + zone limitrofe	5	9	1
Primaria Ricciotti	Via Fosse Ardeatine	1	6	1
Infanzia Calvosa	Via Fonte Corina + zone limitrofe	2	11	1
Primaria Maiuri	Via Tevere	1	11	1
Infanzia Arno	Via Arno	1	6	1
Infanzia Polledrara	Via Tommaso Landolfi	0	1	0
Primaria Cavoni	Viale Madrid + zona cavoni	12	29	2
Liceo Maccari	Piazza Diamanti + zone limitrofe	2	8	0
Primaria Rinascita	Piazza San Pio	2	12	1
		68	**333**	**43**

Di seguito si riportano tutte le installazioni delle antenne settoriali:

Posizionamento	Indirizzo	Q.tà
Palazzo Comunale	Via del Plebiscito	2
Sede Comunale Centro	Piazza VI Dicembre	3
Liceo Turriziani	Via Acciaccarelli	2
Liceo Maccari	Piazza Diamnati	1
Cimitero	Via De Carolis	1
Prefettura	Piazza della Libertà	4
Palazzo Tiravanti	Viale Mazzini	2
Villa Comunale	Via Marco Tullio Cicerone	1
Primaria Via Verdi	Via Verdi	1
Corso Lazio	Corso Lazio	2
Torre Acea	Selva dei Muli	1
Stadio Benito Stirpe	Viale Olimpia	2
		22

Dati e Valutatori

Ente: Comune di Frosinone

Sezione: CED

Redattore e Valutatore dell'Analisi: Ing. Sandro Ricci e Luca Baldassarre

DPO Comune Frosinone: Avv. Matteo Maria Perlini

DPO Comune Frosinone: Stato Valutazione 100%

- Validazione Analisi dei rischi
- Validazione Piano d'azione

Principi fondamentali

Nessuna azione/misura correttiva

Misure esistenti o pianificate

Nessuna azione/misura correttiva

Rischi

Nessun piano d'azione registrato.

Validazione

DPO e parere degli interessati

Nome del DPO/RPD

Avv. Matteo Maria Perlini

Posizione del DPO/RPD

Il trattamento può essere implementato.

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. Inoltre, è un trattamento finalizzato alla sicurezza urbana attuato con modalità analoga a quanto giàeffettuato in numerosissimi contesti analoghi.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento è relativo a filmati effettuati con dispostivi per l'acquisizione di immagini bidimensionali in sequenza, telecamere, per le seguenti finalità:
a. attivare misure di prevenzione e sicurezza sul territorio Comunale;

b. la protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e sicurezza pubblica, la prevenzione, accertamento o repressione dei reati o esecuzione di sanzioni penali a norma del D.Lgs. 51/2018;

c. prevenire eventuali atti di vandalismo o danneggiamento agli immobili ed in particolare al patrimonio comunale e di disturbo alla quiete pubblica;

d. la protezione della proprietà;

e. le attività di rilevazione, prevenzione e controllo delle infrazioni, nel quadro delle competenze attribuite dalla legge;

f. l'acquisizione di fonti di prove in ambito delle attività di polizia amministrativa;

g. per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;

h. monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;

i. verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti

Quali sono le responsabilità connesse al trattamento?

Il titolare è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali. Nello specifico gli obblighi sono:

- trattamento dei dati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- divieto di trattamento dei dati ex art. 9 tranne nei casi di esenzione;
- informare correttamente e in maniera trasparente gli interessati;
- garantire il rispetto dei diritti degli interessati;
- adottare le misure tecniche e organizzative adeguate a garantire, sin dalla fase della progettazione e per impostazione predefinita (privacy by design e by default), la tutela dei diritti dell'interessato e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente;
- vincolo al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;
- fornire le istruzioni al responsabile del trattamento;
- tenere il registro dei trattamenti;
- fornire le istruzioni e formare il personale;
- documentare la violazione dei dati personali, notificarle al Garante e comunicarle agli interessati nei casi previsti;
- cooperare con l'autorità di controllo quando richiesto;
- redigere le valutazioni di impatto nei casi previsti;
- nominare il DPO.

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	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.

	protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia"	
DM del Ministro dell'Interno del 09/08/2008	Ministero dell'interno - Decreto 5 agosto 2008 Incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione. (GU Serie Generale n.186 del 09-08-2008)	Incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione.
D.L. 11/2009	Decreto-Legge 23 febbraio 2009, n. 11 recante "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché' in tema di atti persecutori." convertito con modificazioni dalla L. 23 aprile 2009, n. 38 (in G.U. 24/04/2009, n. 95)	Misure in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché' in tema di atti persecutori.
D.L. 14/2017	Decreto-Legge 20 febbraio 2017, n. 14 recante "Disposizioni urgenti in materia di sicurezza delle città", convertito con modificazioni dalla L. 18 aprile 2017, n. 48 (in G.U. 21/04/2017, n. 93).	Disposizioni in materia di sicurezza delle città
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.P.R.. 22 giugno 1999, n. 250	Regolamento recante norme per l'autorizzazione alla installazione e all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, a norma dell'articolo 7, comma 133-bis , della legge 15 maggio 1997, n. 127.	Regolamento recante norme per l'autorizzazione alla installazione e all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato
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
Art.13, L. 689/1981	Legge 24 novembre 1981, n. 689 recante "Modifiche al sistema penale".	Accertamento delle violazioni amministrative
Artt. 192, 255 e 256 del D.Lgs. 152/2006	Decreto Legislativo 3 aprile 2006, n. 152 recante "Norme in materia ambientale".	Norme in materia ambientale

Ci sono standard applicabili al trattamento?

L'utilizzo dei sistemi della videosorveglianza viene attuato attraverso un corretto impiego delle applicazioni e nel rispetto dei principi applicabili al trattamento di dati personali di cui all'art. 5 dell'RGPD:

1. liceità, quale rispetto della normativa: il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Esso, infatti, è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui i Comuni e l'ufficio di Polizia Locale sono investiti.
2. proporzionalità, con sistemi attuati con attenta valutazione: nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento;

3. finalità, attuando il trattamento dei dati solo per scopi determinati ed espliciti. È consentita la videosorveglianza come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del Titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti;
4. necessità, con esclusione di uso superfluo della videosorveglianza: i sistemi di videosorveglianza sono configurati per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Inoltre, ai sensi del Art. 32 del RGPD, per effettuare il trattamento devono essere adottate misure tecniche ed organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio, lo stesso articolo fissa alcuni principi fondamentali. In particolare, le misure di sicurezza devono essere approntate tenendo conto dei seguenti criteri:

1. lo stato dell'arte;
2. i costi di attuazione;
3. la natura, l'oggetto, il contesto e le finalità del trattamento e
4. il rischio di varia probabilità e gravità di compressione o violazione dei diritti e delle libertà delle persone fisiche.

Le misure di sicurezza devono essere adeguate; è imposta quindi un'obbligazione di mezzi (non di risultato), in modo che siano ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi.

Gli standard internazionali relativi alla sicurezza delle informazioni indicano che la sicurezza dei dati non riguarda solo l'aspetto informatico del trattamento, ma anche l'aspetto organizzativo, a coprire eventi quali la sottrazione o la perdita dei dati e ogni altro evento che possa non renderli disponibili e/o alterarli. Le misure di sicurezza, quindi devono garantire che:

- i dati possano essere consultati, modificati, divulgati o cancellati solo dalle persone autorizzate a farlo (e che tali persone agiscono solo nell'ambito dell'autorità che gli viene concessa);

- i dati trattati siano accurati e completi in relazione alle finalità per cui sono trattati;
- i dati rimangano accessibili e utilizzabili, cioè, in caso di perdita, modifica o distruzione accidentale, si deve essere in grado di recuperarli e prevenire danni alle persone interessate, predisponendo un opportuno piano di continuità operativa.

La predisposizione delle misure di sicurezza richiede che il titolare sia a conoscenza dell'architettura informatica, del luogo e dei supporti con cui sono trattati i dati personali, informazione senza le quali non è possibile definire e implementare misure adeguate.
Le misure di sicurezza si dividono in due categorie: misure organizzative e misure tecniche, che, sempre secondo l'art. 32, comprendono, tra le altre:

- misura tecnica
  a) la pseudonimizzazione e la cifratura dei dati personali;
- requisiti di sicurezza
  b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Valutazione: Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Sono trattati sequenze di immagini (filmati) relative alle aree sottoposte a monitoraggio.
Il trattamento è relativo a filmati effettuati con dispostivi per l'acquisizione di immagini bidimensionali in sequenza, telecamere, per le seguenti finalità:
a. attivare misure di prevenzione e sicurezza sul territorio Comunale;

b. la protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e sicurezza pubblica, la prevenzione, accertamento o repressione dei reati o esecuzione di sanzioni penali a norma del D.Lgs. 51/2018;

c. prevenire eventuali atti di vandalismo o danneggiamento agli immobili ed in particolare al patrimonio comunale e di disturbo alla quiete pubblica;

d. la protezione della proprietà;

e. le attività di rilevazione, prevenzione e controllo delle infrazioni, nel quadro delle competenze attribuite dalla legge;

f. l'acquisizione di fonti di prove in ambito delle attività di polizia amministrativa;

g. per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;

h. monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;

i. verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;

I filmati si riferiscono a persone che transitano e sostano in queste aree.

Oltre ai dati relativi alle immagini sono trattati i relativi metadati (ora e posizione)..

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

Per ciclo di vita del dato s'intende l'insieme delle fasi in cui un dato si può trovare durante la sua esistenza ovverosia:

a) **la raccolta**: il ciclo di vita inizia con la raccolta delle informazioni. I dati possono entrare nel perimetro comunale;

b) **il salvataggio**: una volta che i dati sono entrati all'interno del perimetro comunale dovranno essere memorizzati in appositi luoghi fisici e/o virtuali in modo tale che poi possano essere utilizzati;

c) **l'analisi**: in questa fase si analizzano gli esiti dell'attività di raccolta per determinare la qualità dei dati da utilizzare. Vi è quindi un confronto tra output desiderato e output effettivo per, eventualmente, pianificare migliorie e attività correttive che abbiano impatti sulle fasi precedenti;

d) **il filtraggio dei dati**: in seguito agli esiti dei risultati della fase c), i dati vengono filtrati in modo da rispecchiare gli output desiderati;

e) **l'utilizzo**: in questa fase i dati vengono effettivamente utilizzati per comminare le sanzioni amministrative;

f) **l'archiviazione**: in questa fase i dati vengono memorizzati in attesa di essere dismessi e/o riutilizzati;

g) **la cancellazione o anonimizzazione**: in questa fase il periodo di conservazione è ormai scaduto e quindi: o si cancella il dato personale, oppure lo si rende anonimo. Deve essere evitato, in questa fase, ricorso alla pseudonimizzazione, che porterebbe, come noto, a generare dati destinati ad essere trattati al pari dei personali.

Quali sono le risorse di supporto ai dati?

Supporti digitali conservati in server NVR. Solitamente, ci si avvale di server ubicati presso il comune di Frosinone, che permettono la condivisione e organizzazione dei compiti assegnati.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità di utilizzo dell'impianto di videosorveglianza sono relative alle funzioni istituzionali demandate ai Sindaci ed ai Comuni:
a. dal decreto-legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 "disposizioni urgenti in materia di sicurezza delle città";
b. dal D.Lgs. 18 agosto 2000, n. 267, dal D.P.R. 24 luglio 1977, n. 616;
c. dalla legge sull'ordinamento della Polizia Locale 7 marzo 1986, n. 65 nonché dallo Statuto Comunale e dai Regolamenti Comunali vigenti; d. dal D.lgs. 152/2006 del Codice dell'ambiente;
e possono essere così riassunte:
a. attivare misure di prevenzione e sicurezza sul territorio Comunale;

b. la protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e sicurezza pubblica, la prevenzione, accertamento o repressione dei reati o esecuzione di sanzioni penali a norma del D.Lgs. 51/2018;
c. le attività di rilevazione, prevenzione e controllo delle infrazioni, nel quadro delle competenze attribuite dalla legge;
d. l'acquisizione di fonti di prove in ambito delle attività di polizia amministrativa;
e. per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
f. monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
g. verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;
Si precisa che tra le finalità di utilizzo dell'impianto non sono comprese quelle dell'art. 4 dello Statuto dei lavoratori (legge 300 del 20 maggio 1970) relative al controllo a distanza dell'attività dei lavoratori per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento, ai sensi dell'articolo 6, comma 1, lettera e) del Regolamento (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 del Trattamento ed il Comandante del Comando di Polizia Locale del comune di Frosinone ossia finalizzato alla prevenzione reati ed illeciti amministrativi nonché contrastare l'abbandono di rifiuti e monitorare le aree di proprietà del comune di Frosinone al fine di individuare gli eventuali trasgressori.

In particolare il riferimento normativo è di individuare nell'art. 54 del D.Lgs. 267/2000 relativo alle Attribuzioni del sindaco nelle funzioni di competenza statale e alle disposizioni contenute nell'articolo 6, commi 7 e 8, del decreto-legge 23 febbraio 2009, secondo le quali i comuni possono utilizzare i sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per finalità di tutela della sicurezza urbana e la conservazione dei dati, delle informazioni e delle immagini raccolte è limitata ai sette giorni successivi alla rilevazione avvenuta a mezzo di tali sistemi, fatte salve speciali esigenze di ulteriore conservazione

Valutazione: Accettabile

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 raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati) in quanto il trattamento delle immagini acquisite attraverso l'utilizzo del sistema di videosorveglianza è effettuato solo in aree in cui non risulta possibile il ricorso a strumenti e sistemi di controllo alternativi anche per limitatezza delle risorse umane che possono essere adibite all'effettuazione dei controlli necessari a garantire la sicurezza urbana,
Si consideri che le disposizioni legislative in materia di sicurezza attribuiscono ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidate ad essi dalla legge in materia di sicurezza e di polizia giudiziaria.

Inoltre, al fine di prevenire e contrastare determinati pericoli che minacciano l'incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell'ordinamento.
Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le Forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'interno.
Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di video sorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana.

L'effetto deterrente costituito dalla presenza di un sistema di videosorveglianza ha fatto registrare evidenze significative.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

I dati sono intrinsecamente esatti e aggiornati in quanto acquisiti in modo automatico attraverso dispostivi (telecamere) per l'acquisizione di immagini bidimensionali in sequenza e vengono scaricati dal server solo nel caso venga rilevata una condotta illecita.

Nel suddetto caso viene espletata l'attività di accertamento dell'illecito facendo uso dei filmati scaricati dal sistema.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Per le immagini che non documentano un fatto illecito il periodo massimo di conservazione di dati è di 7 giorni.
Nel momento in cui se ne presenti l'esigenza a fronte di una segnalazione e/o fronte della constatazione di un atto vandalico o altro fatto illecito un addetto autorizzato al trattamento visiona i firmati registrati;
Nel caso vengano individuate immagini che documentano visivamente un fatto illecito la sequenza delle immagini a esso riferito vengono scaricate in un'apposita cartella protetta del Server.
Per quanto riguarda i filmati che vengono scaricati per effettuare l'accertamento delle violazioni il periodo di conservazione è limitato alle esigenze di conservazione dei filmati ai fini della composizione del fascicolo utile alla definizione del procedimento.

Il fascicolo viene consegnato con modalità sicure al soggetto che avvia e svolge il procedimento amministrativo o penale, al termine di tale operazione i documenti sono cancellati in modo irreversibile.

Valutazione: Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

1) In conformità alle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati (European Data Protection Board) e a quanto disposto degli artt. 13-14 dell'RGDP è adottato un approccio scalare, attraverso una combinazione di metodi al fine di assicurare la trasparenza che prevede:
a. una segnaletica di avvertimento nei pressi delle telecamere (primo livello);
b. un'informativa di dettaglio fornita attraverso una pagina internet dove sono disponibili le informazioni di secondo livello (secondo livello).

2) Le informazioni di primo livello sono posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi).

Non è rivelata l'ubicazione della telecamera ma l'interessato è messo nelle condizioni di stimare quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.

Le informazioni fornite esplicitano: le finalità del trattamento, l'identità del Titolare del trattamento e l'esistenza dei diritti dell'interessato, la base giuridica del trattamento e i recapiti del responsabile della protezione dei dati, la trasmissione dati a terzi, il periodo di conservazione oltre all'indicazione della pagina internet dove sono disponibili le informazioni di secondo livello.

Per la segnaletica di avvertimento è utilizzato un modello conforme al fac-simile riportato sulle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati (European Data Protection Board)
In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, sono installati più cartelli.
La segnaletica di avvertimento nei pressi delle telecamere (primo livello) nello specifico:
• è collocata prima del raggio di azione della telecamera, nelle sue immediate vicinanze;
• ha un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza è attivo in orario notturno;
• ingloba un simbolo stilizzato di esplicita e immediata comprensione.

3) Le informazioni di secondo livello sono facilmente accessibili per l'interessato e messi a disposizione attraverso la pagina internet indicata sull'informativa di primo livello e contengono tutti gli elementi obbligatori a norma dell'art. 13 dell'RGPD e dell'art.10 D.Lgs. 51/2018.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Non è richiesto il consenso degli interessati, la base giuridica del trattamento è la lettera e) dell'art. 6 del Reg. (UE) 2016/679: "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;".

Nel caso in cui la violazione rilevata comporta una sanzione penale non è richiesto il consenso in quanto il titolo giuridico del trattamento è il comma 1 dell'art.5 del D.Lgs. 51/2018.

Valutazione: Accettabile

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

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.
Con i cartelli informativi posizionati a debita distanza dal "cono di ripresa", nonché attraverso l'informativa pubblicata sul sito istituzionale del comune di Frosinone, l'interessato viene messo a conoscenza delle del fatto che, in qualunque momento, può 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.
Per quanto riguarda i trattamenti effettuati ai sensi del D.Lgs. 51/2018 il diritto di accesso è esercitabile ai sensi dell'art.11 del D.Lgs. 51/2018 non è previsto il diritto alla portabilità per i trattamenti effettuati ai sensi del D.Lgs. 51/2018.

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.
Con i cartelli informativi posizionati a debita distanza dal "cono di ripresa", nonché attraverso l'informativa pubblicata sul sito istituzionale del comune di Frosinone, l'interessato viene messo a conoscenza delle del fatto che, in qualunque momento, può 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.
Con i cartelli informativi posizionati a debita distanza dal "cono di ripresa", nonché attraverso l'informativa pubblicata sul sito istituzionale del comune di Frosinone, l'interessato viene messo a conoscenza delle del fatto che, in qualunque momento, può 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 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.).
Per quanto riguarda i trattamenti effettuati ai sensi del D.Lgs. 51/2018 i diritti rettifica e cancellazione sono esercitabili ai sensi dell'art.12 del D.Lgs. 51/2018.

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.

Con i cartelli informativi posizionati a debita distanza dal "cono di ripresa", nonché attraverso l'informativa pubblicata sul sito istituzionale del comune di Frosinone, l'interessato viene messo a conoscenza delle del fatto che, in qualunque momento, può 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.

Con i cartelli informativi posizionati a debita distanza dal "cono di ripresa", nonché attraverso l'informativa pubblicata sul sito istituzionale del comune di Frosinone, l'interessato viene messo a conoscenza delle del fatto che, in qualunque momento, può 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.

Per quanto riguarda i trattamenti effettuati ai sensi del D.Lgs. 51/2018 il diritto di limitazione è esercitabile ai sensi dell'art.14 del D.Lgs. 51/2018.

Valutazione: Accettabile

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

Nel caso si rilevi necessario fare ricorso ad un responsabile esterno del trattamento gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati con atto di nomina (contrato) ai sensi e per gli effetti del art. 28 Reg. UE 2016/679.
Ogni contratto definisce la tipologia del trattamento e dati trattati e con riferimento agli obblighi inerenti al mandato del Responsabile lo impegna ad adottare tutte le misure necessarie all'attuazione delle disposizioni di legge contenute nel Reg.to Europeo 2016/679. Il contratto definisce dello specifico:
- i termini relativi al trattamento dei dati;
- le modalità di comunicazione di dati;
- le misure per garantire l'affidabilità del trattamento e la non divulgazione dei dati;
- le misure tecniche ed organizzative adeguate a garantire la sicurezza del trattamento;
- la catena delle responsabilità;
- i diritti degli interessati;
- le modalità di gestione delle eventuali violazione dei dati personali;
- la collaborazione richiesta per l'effettuazione della valutazione d'impatto sulla protezione dei dati personali;
- le modalità operative per la cancellazione o la restituzione dei dati;
- il diritto di audit del titolare nei confronti del responsabile;
- le modalità per un eventuale trasferimento di dati personali da parte del Responsabile nei confronti di un Sub responsabile;
- l'impegno all'adozione e rispetto di codici di condotta e certificazioni;
- una serie di condizioni generali.

Valutazione: Accettabile

Piano d’azione/misure correttive:

Nessun piano d’azione/misura correttiva

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

Controllo degli accessi logici

L'accesso è controllato da password di lunghezza minima di 8 caratteri composta da lettere, numeri e caratteri speciali. Le password vengono modificate periodicamente ai fini di garantire un accesso sicuro.

Valutazione: Accettabile

Tracciabilità

Le immagini vengono archiviate per il tempo necessario su un NAS server dedicato con l'indicazione di orario, data e luogo.

Valutazione: Accettabile

Archiviazione

Tutta la documentazione digitale relativa all'attività di rilevazione di filmati/ immagini è salvata su NAS server dedicato nonchè regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per gli enti pubblici

Valutazione: Accettabile

Minimizzazione dei dati

I dati vengono trattati e archiviati in forma minima, in quanto l'ente detiene soltanto il frame che ritrae l'abbandono dei rifiuti.

Valutazione: Accettabile

Gestione postazioni

Ogni postazione è dotata di un pc con relativa password alfanumerica che viene modificata periodicamente ai fini di garantire un accesso sicuro.

Valutazione: Accettabile

Vulnerabilità

I software utilizzati per la trasmissione dei dati sono costantemente aggiornati. I filmati/immagini possono essere visionati solo con l'ausilio di un software licenziato con autenticazione con chiave di cifratura esadecimale. Gli apparecchi utilizzati sono soggetti a revisione periodica.

Valutazione: Accettabile

Lotta contro il malware

I sistemi informatici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus). È stato, inoltre, fornito agli utilizzatori delle linee guida sull'utilizzo sicuro delle risorse elettroniche e digitali, che includano le istruzioni per una efficace lotta al malware.

Valutazione: Accettabile

Manutenzione

Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware e software del comune di Frosinone.

Valutazione: Accettabile

Sicurezza dei canali informatici

Rete intranet dell'ente. Firewall, antivirus perimetrale, accesso tramite autenticazione su Domain Controller

Valutazione: Accettabile

Controllo degli accessi fisici

L'accesso ai NAS server dedicati è consentito solo al personale autorizzato.

Valutazione: Accettabile

Sicurezza dell'hardware

I server NAS sono ubicati in un ambiente dedicato esclusivamente ai medesimi e tenuti sotto chiave all'interno di una stanza singola con sistema di aerazione, porta blindata, videosorveglianza interna e esterna sugli accessi, in cui vi può accedere solo personale dipendente autorizzato.

Valutazione: Accettabile

Prevenzione delle fonti di rischio

Misure sia fisiche, logiche e organizzative.

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

Il titolare del trattamento 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.
Il titolare al momento dispone di un impianto documentale relativo alle misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.

Valutazione: Accettabile

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

Rischi Accesso

Accesso illegittimo ai dati

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

Violazione della riservatezza di dati personali comuni e/o sensibili, comunicazione/diffusione dei dati non autorizzata, conoscenza da parte di terzi del fatto che è stata posta in essere una condotta costituente illecito amministrativo, interferenza su abitudini, interferenza su vita privata

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso abusivo ai sistemi, malware, hacker, cancellazione involontaria, distruzione del dispositivo, furto del dispositivo, cancellazione volontaria

Quali sono le fonti di rischio?

Un soggetto autorizzato che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. Terzi che fanno un accesso abusivo ai sistemi.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Gestione postazioni, Vulnerabilità, Lotta contro il malware, Manutenzione, 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.

La quantità e la rilevanza dei dati personali trattati potrebbe comportare una gravità di rischio che può essere considerata Trascurabile. La divulgazione di dati personali di cui il comune di Frosinone è titolare, anche ex Art. 9 e 10 GDPR, potrebbe avere conseguenze negative sugli interessati.

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

Trascurabile.

L'attivazione di sistemi di vigilanza interna e l'adozione e l'attuazione del regolamento, unito ad attività di sensibilizzazione del personale dipendente, possono essere in grado di limitare violazioni ad alto impatto. La limitazione a priori del trattamento di dati ex Art. 9 e 10, con deroghe in particolari condizioni da parte del titolare, permette di limitare i potenziali rischi connessi ad una loro diffusione illecita.

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 abusivo ai sistemi, hacker, malware, furto del dispositivo

Quali sono le fonti di rischio?

Un soggetto autorizzato che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. Terzi che fanno un accesso abusivo ai sistemi, Errore umano, Fonti umane interne, che intervengano nella modifica dei dati.

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

Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Gestione postazioni, Vulnerabilità, Lotta contro il malware, Manutenzione, 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.

Sebbene la violazione potrebbe portare ad una errata o inefficace prestazione del servizio, le misure di controllo degli accessi logici permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica.

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

Trascurabile,

Appare marginale che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda alla corretta applicazione e gestione delle misure di sicurezze adottate e pianificate dal comune di Frosinone.

Valutazione: Accettabile

Rischi Perdita

Perdita di dati

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

Violazione della riservatezza di dati personali comuni e/o sensibili, indisponibilità dei dati

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

Accesso abusivo ai sistemi, furto del dispositivo, distruzione del dispositivo, cancellazione involontaria, attacco hacker, malware, distruzione dei server del servizio.

Quali sono le fonti di rischio?

Fonti umane interne, fonti umane esterne, eventi naturali che possano influire sui dispositivi fisici di archiviazione

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

Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Gestione postazioni, Vulnerabilità, Lotta contro il malware, Manutenzione, 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.

Appare marginale che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda alla corretta applicazione e gestione delle misure di sicurezza adottate e pianificate dal comune di Frosinone.

Valutazione: Accettabile

Tabella Rischi

Panoramica dei rischi

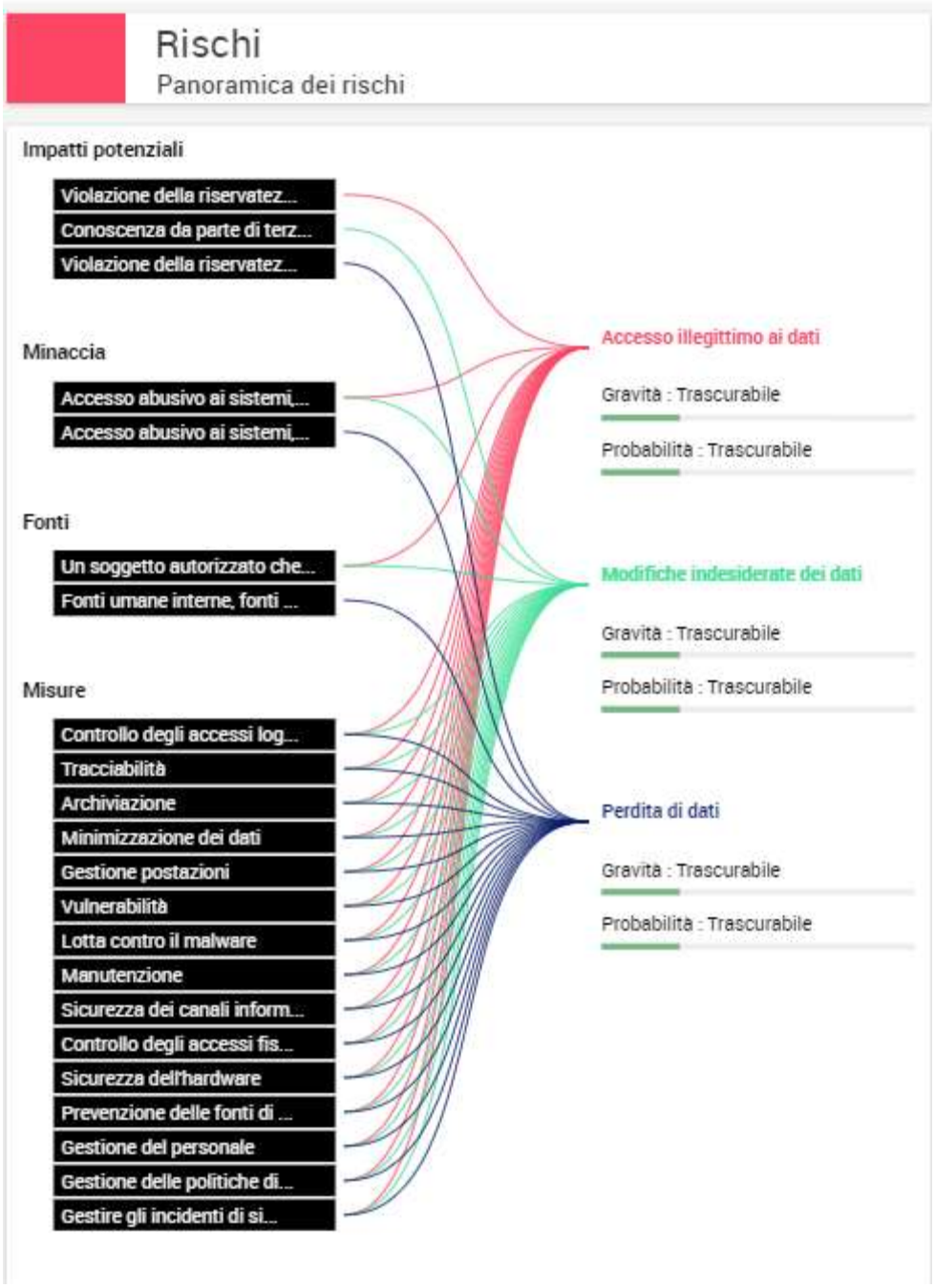
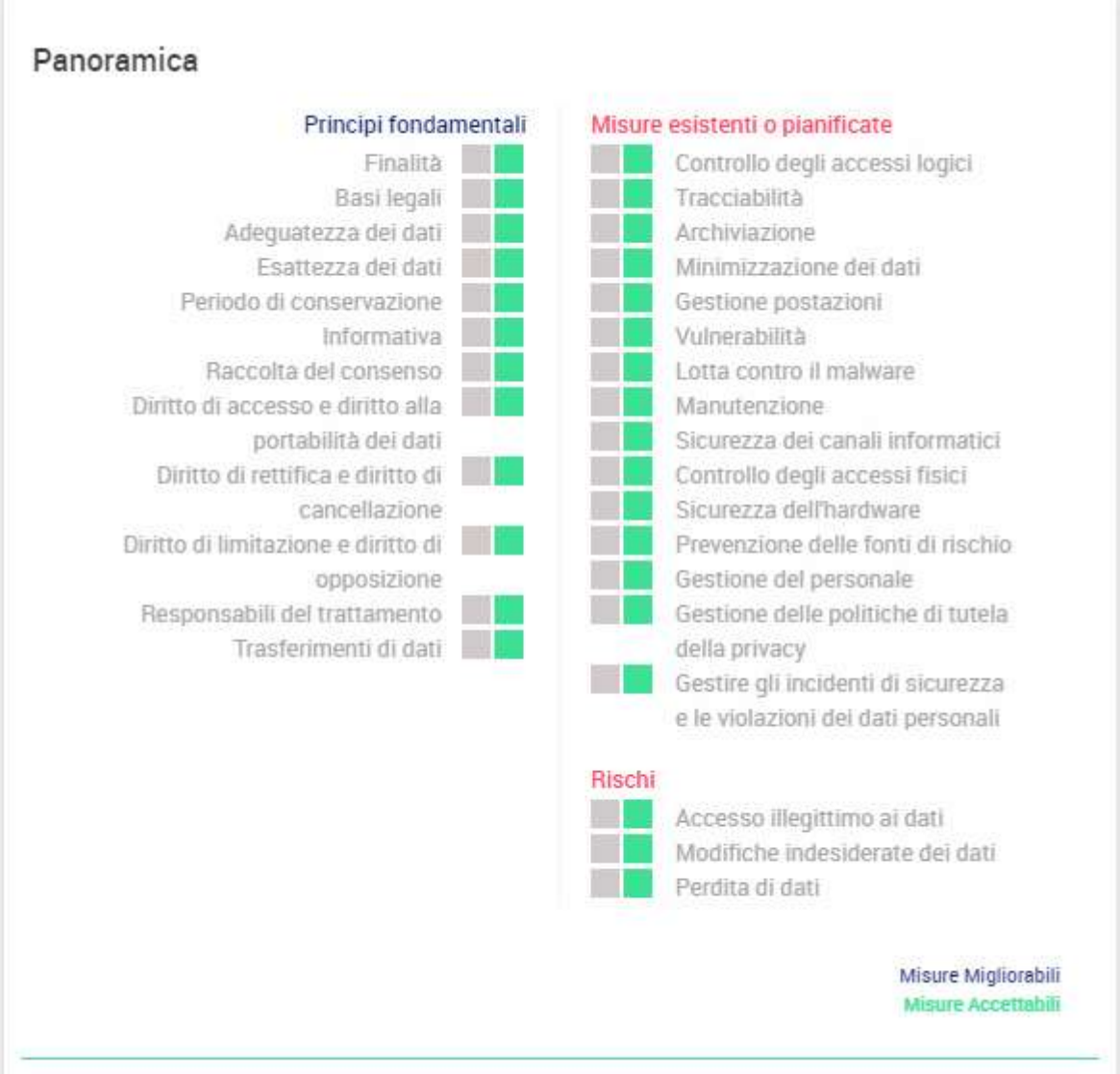


Tabella Gravità del Rischio

- 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



Frosinone, 19 gennaio 2023

Il Responsabile
Ing. Sandro Ricci

Il DPO
Avv. Matteo Maria Perlini

PERLINI MATTE
2023.01.31 11:08:26
CN=PERLINI MATTEO MA
C=IT
O=ORDINE DEGLI AVVOC
2.5.4.97=VATIT-800114506
RSA/2048 bits