COMUNE DI NEVIANO

(*Provincia di Lecce*)

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI AI SENSI DEL REGOLAMENTO UE 2016/679, IN RELAZIONE AL TRATTAMENTO DI DATI EFFETTUATO TRAMITE I SISTEMI DI VIDEOSORVEGLIANZA COMUNALI .

Approvata con Delibera di Giunta n.127 del 17/11/2025

Sommario

Informazioni sulla DPIA ..... **Errore. Il segnalibro non è definito.**
Contesto 4
Panoramica del trattamento 4
Dati, processi e risorse di supporto 7
Principi Fondamentali 9
Proporzionalità e necessità 9
Misure a tutela dei diritti degli interessati 13
Rischi 16
Misure esistenti o pianificate 16
Metodo adottato per l'analisi dei rischi 24
Accesso illegittimo ai dati 26
Modifiche indesiderate dei dati 29
Perdita di dati 32
Piano d'azione 34
Principi fondamentali 34
Misure esistenti e pianificate 36
Rischi 38
Pareri 39
Parere DPO/RPD 39
Parere degli interessati 39

INFORMAZIONI SULLA DPIA

Nome della valutazione d'impatto

Valutazione di impatto relativa al "**SISTEMA DI VIDEOSORVEGLIANZA INTEGRATA PER LA SICUREZZA URBANA**" del Comune di Neviano.

Nome autore

- Il Comandante della Polizia Locale, Comm. Romeo Dott. Antonio Angelo, in qualità di Designato interno ai sensi dell'art. 2-quaterdecies del D. Lgs. 196/2003 e delegato del Titolare del Trattamento.
- Dott. Ing. Davide Fortunato.

Titolare del trattamento

Il COMUNE DI NEVIANO, rappresentato dal Sindaco Giuseppe Antonio Mighali.

Data

14/11/2025

Allegati:

1) Relazione tecnica illustrativa
2) Planimetrie di dettaglio delle postazioni
3) Patto per la sicurezza urbana

CONTESTO

Panoramica del trattamento

Il presente documento contiene una valutazione di impatto sulla protezione dei dati personali, relativamente al trattamento derivante dai sistemi di "VIDEOSORVEGLIANZA INTEGRATA PER LA SICUREZZA URBANA".

Il trattamento dei dati personali è effettuato a seguito dell'attivazione e implementazione di una serie di impianti/sistemi/presidi di videosorveglianza installati sul territorio cittadino o presso strutture di rilevante valore storico-artistico. La disponibilità tempestiva di immagini presso il Comando della Polizia Locale dove i monitor ed il server/NVR è ubicato, costituisce uno strumento di prevenzione e contrasto della criminalità diffusa e predatoria (in aree maggiormente interessate da situazioni di degrado e di illegalità) e di razionalizzazione dell'azione delle pattuglie dislocate sul territorio comunale, anche in raccordo con altre Forze dell'Ordine e da quanto stabilito nel "Patto per l'attuazione della Sicurezza Urbana" siglato con la Prefettura; attraverso tali strumenti l'Ente persegue l'intento di tutelare la popolazione e 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, negli ambienti in prossimità delle scuole e nelle strade interessate da un particolare traffico veicolare.

A tal fine il Comune dispone l'utilizzo del sistema di videosorveglianza in dotazione alla Polizia Locale, ai fini di prevenzione e repressione di atti delittuosi anche nell'ambito del più ampio concetto di "sicurezza urbana", così come 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 videosorveglianza comporta 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 nelle aree interessate.

Le operazioni di trattamento dati che il Comune di NEVIANO esegue sul territorio attraverso i sistemi di videosorveglianza attualmente esistenti, perseguono le seguenti finalità (come nel seguito del documento meglio specificate):

- prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria;
- promozione del rispetto del decoro urbano;
- vigilanza sulla sicurezza stradale e della mobilità veicolare e pedonale;
- svolgimento di funzioni di pubblica sicurezza;
- vigilanza e prevenzione reati ed illeciti;
- attività di polizia giudiziaria (i sistemi OCR verificano il passaggio di autoveicoli rubati).

La presenza di una rete funzionante di telecamere, infatti, è stata implementata quale deterrente per condotte criminali, pericolose o scorrette, atti vandalici, prevenzione e contrasto alle forme di illegalità presenti nel territorio quali piazze, strade di accesso all'abitato, tutela dei beni di maggiore pregio, parchi urbani, fenomeni di abusivismo commerciale, occupazioni abusive, etc.

Si tratta di uno strumento di supervisione, documentazione e coordinamento ad uso del Comando di Polizia Locale e delle Forze dell'Ordine.

L'attività di videosorveglianza eseguita dal Comune è, pertanto, esercitata per lo svolgimento di funzioni e poteri pubblici e 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.

Attualmente il sistema si compone di n. 15 telecamere connesse alla sala di controllo posta presso il Comando della Polizia Locale. Il sistema è a circuito chiuso e il relativo elaboratore è connesso da un

server ubicato in Questura di Lecce, dove avviene la visualizzazione delle sole telecamere lettura targhe.
Elenco siti delle n. 11 telecamere di sicurezza del territorio (c.d. contest, del tipo Bosch mod. telecamera BULLET DINION IP 3000i 5MP obiettivo motor. 3,2-10mm h.265 12VDC) e n. 4 telecamere di lettura targhe (del tipo TARGASYSTEM TS3MPX-OCR doppia corsia 5MPX):

Elenco siti telecamere di sicurezza del territorio:

- Via Degli Ulivi (Campo sportivo)
- Via Regina Elena
- Via Roma
- Piazza Concordia
- Via Dante (Municipio)
- P.le Manuel Florito (Parco croce)
- Via Kennedy (area mercatale)
- Via XXV Maggio (mercato coperto)
- Via Giovanni XXIII (poliambulatorio)
- Via Graziani ang. via Umberto I
- Via Giovanni XXIII (anfiteatro/parco)

Elenco siti telecamere di lettura targhe:

- Ingresso Collepasso (via Rondò-via Graziani)
- Ingresso Tuglie (via Tuglie - via Umberto I)
- Ingresso via vecchia di Parabita
- Ingresso Seclì (via Roma)

Si tratta di telecamere intelligenti (*in quanto riconoscono marca, modello, colore e classe ambientale dei veicoli*) fisse posizionate nell'area urbana e nel territorio, finalizzata al presidio del territorio stesso.

Tutti gli impianti vengono gestiti a livello centralizzato, con server/NVR e monitor per la rilevazione ed estrazione delle immagini, collocati nella Control room presso la Sede Municipale, accessibile solo al Comandante della Polizia Locale e persone dallo stesso appositamente delegate.
La rete è separata da quella del Comune e collegata tramite una linea internet dedicata, attraverso una rete VPN ad un server in Questura di Lecce, dove avviene l'invio delle letture delle targhe al server in questione; il sistema funziona mediante collegamento dati da antenne.

L'analisi dello scenario di riferimento, volto alla valutazione dei rischi pendenti sui diritti e le libertà delle persone fisiche, è stata eseguita seguendo il Provvedimento dell'Autorità Garante per la protezione dei dati personali del 8 aprile 2010, le linee guida predisposte dal Gruppo di lavoro ex art. 29, ora European Data Protection Board, completate dalle metodologie indicate dalle norme tecniche ISO 31000 e ISO 29134, le "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video" dell'EDPB.

La presente valutazione di impatto, pertanto, viene effettuata su tutti i sistemi di videosorveglianza comunali, in quanto trattasi di sorveglianza sistematica su larga scala di zone accessibili al pubblico.

Quale è il trattamento in considerazione?

Le operazioni di trattamento dati che il Comune di Neviano esegue sul territorio attraverso i diversi sistemi di videosorveglianza, perseguono le seguenti finalità:

1. Attivazione di misure di prevenzione e "sicurezza urbana" sul territorio comunale, garantendo maggiore sicurezza ai cittadini conformemente al Decreto Ministro Interno 5 Agosto 2008;
2. Attivazione di uno strumento operativo di protezione civile sul territorio urbano;

3. Rilevazione di dati anonimi per l'analisi dei flussi di traffico e per la predisposizione dei piani comunali del traffico;
4. Vigilare sulla circolazione stradale, rilevando le targhe identificative dei veicoli transitanti nel territorio comunale, ai fini del controllo statistico e della sicurezza;
5. Tutela del patrimonio comunale, prevenzione e repressione di atti vandalici o di teppismo in luoghi pubblici;

Il Titolare del trattamento ha disposto, pertanto, nel rispetto della vigente normativa in materia e delle prescrizioni fornite dal Garante per la protezione dei dati personali, l'attivazione di un impianto di videosorveglianza urbana mediante l'installazione di telecamere/ fotocamere debitamente segnalate.
Le apparecchiature sono indirizzate verso aree pubbliche o soggette a servitù di pubblico passaggio nonché su beni di proprietà comunale, individuati in ragione delle esigenze di sicurezza delle persone fisiche, tutela della sicurezza stradale e tutela del patrimonio comunale.
Il trattamento dei dati personali preso in considerazione nella presente valutazione d'impatto è quello realizzato mediante impianti di videosorveglianza attivati nel territorio del Comune, che consentono la visione in diretta delle immagini riprese dalle telecamere e i dati personali rilevati mediante le riprese video che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti e i mezzi di trasporto che transiteranno nell'area interessata.
Tali impianti sono collegati ai locali della Polizia Locale e alle postazioni di lavoro del Comandante.
I punti di osservazione sono costituiti da telecamere in installazione su palo o parete con registrazione di immagini e dati e il cui trattamento sarà eseguito dagli operatori della Polizia Locale.
Il trattamento preso in considerazione consiste, pertanto, in riprese video nell'ambito di varie attività dell'Ente fra cui:

1. videosorveglianza con funzioni di sicurezza urbana, ordine e sicurezza pubblica, prevenzione, accertamento e repressione dei reati, episodi di criminalità diffusa e/o predatoria, protezione e tutela del patrimonio;
2. controllo della circolazione veicolare;

Quali sono le responsabilità connesse al trattamento?

I soggetti coinvolti nell'attività di trattamento sono:

a) il Comune di NEVIANO (Titolare del trattamento), nella persona del Sindaco, che ha delegato il Comandante della Polizia Locale quale Designato ex art. 2-quaterdiecies del D. Lgs. 196/2003;
b) Utenti autorizzati (*per la visualizzazione ed estrazione è competente solo il Comandante, che potrà eventualmente delegare specifiche persone autorizzate*);
c) la società esterna che ha implementato il sistema di videosorveglianza (*Facegroup Srl, con sede in Squinzano in Via G. Lamarmora, 80*) ed effettua attività di manutenzione su tali sistemi di videosorveglianza, mediante accesso ai dati (*anche da remoto*), responsabile dell'implementazione delle misure di sicurezza.

Come detto, il Titolare del trattamento è il Comune di NEVIANO nel suo complesso, che opera tramite i propri uffici e servizi deputati alle varie attività, in collaborazione anche con istituzioni esterne (es. Autorità di sicurezza o Forze di Polizia) ed eventualmente con altri soggetti (appositamente designati quali Responsabili del trattamento, ex art. 28 del GDPR).
I dati sono resi accessibili (su richiesta) anche alle seguenti categorie di destinatari (che operano in qualità di autonomi titolari del trattamento): Autorità di vigilanza e controllo, Uffici giudiziari, Forze di polizia (come Questura, Carabinieri, Guardia di Finanza, tutti in qualità di autonomi titolari).

Gli uffici dove sono presenti i sistemi di archiviazione delle immagini sono collocati presso la sede del Comando di Polizia Locale; in particolare, tutti gli impianti vengono gestiti a livello centralizzato, con server/NVR chiusi a chiave in un armadio rack e monitor per la rilevazione ed estrazione delle

immagini, posti nella stanza accessibile solo al Comandante della Polizia Locale e personale della Polizia Locale delegato e formalmente autorizzato, nonché con la postazione di lavoro del Comandante.
La rete del sistema di videosorveglianza è separata da quella del Comune e collegata tramite una linea internet dedicata, attraverso una rete VPN ad un server in Questura di Lecce, dove avviene l'invio delle letture delle targhe al server in questione.
A tali strumenti vi può accedere solo il Comandante ed eventualmente solo i soggetti autorizzati che detengono le password per accedere agli strumenti assegnati e alle immagini registrate dagli impianti di videosorveglianza di propria competenza.

Ci sono standard applicabili al trattamento?

Nel trattamento oggetto di valutazione non ci sono specifici standard applicabili al trattamento.
I principali standard sono collegati alle caratteristiche tecniche/tecnologiche dei prodotti. Dal punto di vista del processo/trattamento e degli adempimenti conseguenti, si fa riferimento principalmente a:

- Reg. UE 2016/679 (GDPR) e D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018)
- D.LGS. 51/2018
- CODICE DELLA STRADA E REGOLAMENTI INTERNI ATTUATIVI
- DISPOSIZIONI COMUNALI
- PROVVEDIMENTO DEL GARANTE PRIVACY DELL'8 APRILE 2010
- PARERI E PROVVEDIMENTI GENERALI DEL GARANTE PRIVACY (COMPRESE LE VERIFICHE PRELIMINARI)
- LINEE GUIDA DELL'EDPB 3/2019 sul trattamento dei dati personali attraverso dispositivi video (adottate il 29 gennaio 2020)

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati consistono in immagini e video registrati sul piano operativo (non viene attivata alcuna funzione audio); la registrazione è attiva h 24 e le immagini vengono salvate su apposito server/NVR collocato all'interno del Comando di Polizia Locale e conservate (*per un massimo di 7 giorni*); l'accesso alle immagini è consentito solamente al personale incaricato qualora vi sia una situazione di particolare criticità che necessita la documentazione video degli eventi.
I principali dati trattati sono quindi le immagini, i video e le registrazioni, nonché i dati relativi alle targhe dei veicoli. Gli interessati a cui appartengono i dati sono cittadini, persone fisiche, maggiori o minori d'età e qualunque altro soggetto entri nel raggio d'azione delle videocamere.

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

L'ordinario ciclo di vita del trattamento è sostanzialmente dato:

- RACCOLTA DEI DATI (principalmente automatizzata)
- REGISTRAZIONE E CONSERVAZIONE (principalmente automatizzata, salvo casi particolari)
- ELOBAROZAZIONE (TRAMITE PERSONALE ESPRESSAMENTE AUTORIZZATO)
- ARCHIVIAZIONE PER I TEMPI DEL PROCEDIMENTO IN ESSERE

- ESTRAZIONE delle immagini (a richiesta o in caso di evento)
- DISTRUZIONE/CANCELLAZIONE (automatizzata e/o tramite personale espressamente autorizzato nel caso di procedimenti aperti).

Le immagini riprese dalle telecamere vengono trasmesse attraverso un collegamento alla sala di controllo posta nei locali della Polizia Locale del Comune. Le telecamere consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o, in caso contrario in bianco/nero.
Tali caratteristiche tecniche consentono un significativo grado di precisione e di dettaglio della ripresa.
In questa sede le immagini saranno visualizzate su di un monitor e registrate su di un supporto magnetico.
L'accesso alla sala di controllo è consentito solamente alla persona designata al trattamento dei dati, ai preposti nonché al personale addetto alla manutenzione degli impianti, designato dal responsabile del trattamento. Eventuali accessi di persone diverse da quelli innanzi indicate sono autorizzati per iscritto dal titolare del trattamento.
I monitor degli impianti di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate. 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'accesso alle immagini da parte del designato e di preposti si limita alle attività oggetto della sorveglianza; eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione. In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo. I dati trattati non saranno oggetto di diffusione a terzi, ad eccezione dei casi di espressa e motivata disposizione dell'Autorità giudiziaria.

Quali sono le risorse di supporto ai dati?

Le immagini vengono gestite e registrate da un server. Sia le registrazioni che le immagini trasmesse dalle telecamere al server sono cifrate con software Milestone. Le antenne di trasmissione dati (Force 300-16) dislocate sul territorio comunale hanno anch'esse un sistema di cifratura.
In Questura di Lecce, vi è un server analogo a quello presente presso la Polizia Locale, il quale acquisisce i dati delle lettura targhe, e a sua volta, sarà interconnesso alla banca dati ubicata presso il Sistema Centrale Nazionale Targhe e Transiti (S.C.N.T.T) in uso alle Forze di Polizia presso il Centro Elettronico Nazionle della Polizia di Stato con sede a Napoli.
Per la realizzazione di queste interconnessioni saranno dedicate delle linee internet dedicate, le quali saranno protette da firewall e saranno create delle reti private virtuali che utilizzano la crittografia per codificare i tuoi dati, creando un "tunnel" sicuro attraverso Internet

Le telecamere di lettura targhe sono del tipo TARGASYSTEM TS3MPX-OCR doppia corsia 5MPX, mentre le di contest del tipo Bosch mod. telecamera BULLET DINION IP 3000i 5MP obiettivo motor. 3,2-10mm h.265 12VDC.

Valutazione: Accettabile
Commento di valutazione: l'analisi è ritenuta accettabile. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I sistemi di videosorveglianza in questione sono impiegati unicamente per finalità di sicurezza urbana (di cui agli artt. 4 e 5, co. 2, lett. a), del d.l. 20 febbraio 2017, n. 14) e controllo del territorio.

Oltre a quanto sopra indicato e ai riferimenti di legge, la liceità è altresì 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, quindi, a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia 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 NEVIANO, attraverso il Comando di Polizia Locale, effettua il trattamento di dati personali mediante i nuovi impianti di videosorveglianza urbana per tutelare la sicurezza urbana attraverso azioni volte al:

- perseguimento di finalità di sicurezza urbana ai sensi del D.L. 20 febbraio 2017, n. 14, al fine di garantire il necessario grado di sicurezza dei cittadini e di tutte le persone che fanno parte della comunità;
- prevenzione e contrasto di fenomeni di criminalità diffusa e predatoria;
- promozione del rispetto del decoro urbano e tutela del patrimonio comunale.

In particolare, l'uso di tutti i sistemi e tipologie di videosorveglianza del territorio comunale è finalizzato, in base alle circostanze e ai diversi sistemi utilizzati, 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 videosorveglianza dd. 08/04/2010) o comportamenti in grado di compromettere la sicurezza, la salute e la incolumità delle persone, anche in dipendenza da eventi relativi alla circolazione stradale, commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini (attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale);
c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e a prevenire eventuali atti di vandalismo o danneggiamento;
d) controllo di determinate aree, tutelando in tal modo coloro che più necessitano di attenzione (bambini, giovani e anziani), garantendosi, nel contempo, un elevato grado di sicurezza nelle zone monitorate;
e) monitoraggio del traffico e all'analisi dei flussi di traffico necessari alla predisposizione dei piani del traffico, per una più corretta gestione della mobilità urbana o per statistiche sullo stesso (la vigilanza sul pubblico traffico per consentire l'immediata adozione di idonee contromisure);

f) tutela della sicurezza stradale, per monitorare la circolazione lungo le strade del territorio comunale e fornire ausilio in materia di polizia amministrativa in generale;
g) tutela, in particolare, delle persone che più necessitano di attenzione, come 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 (atti sessuali con minorenni, violenza sessuale di gruppo e atti persecutori);
h) fornire un supporto informativo di ausilio per gli agenti della forza pubblica per tutti i comportamenti posti in violazione della normativa penale;
i) prevenire eventuali atti di vandalismo e/o danneggiamento ovvero spaccio di sostanze stupefacenti in particolari aree.

I sistemi di videosorveglianza utilizzati dal Comune 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. La videosorveglianza territoriale è, quindi, uno strumento funzionale allo svolgimento dei compiti istituzionali del Comune.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Quali sono le basi legali che rendono lecito il trattamento?

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 ovvero in adempimento a obblighi di legge o di regolamento (art. 6, par. 1, lett. c ed e del GDPR, art. 5 e 7 del Dlgs 18 maggio 2018, n. 51 e art. 23, comma 1, del D.P.R. n. 15 del 2018, D.L. 11/2009, 54 D.Lgs. 267/2000, 38 c. 3 D.L. 76/2020 convertito in L. 120/2020, Regolamento comunale).
Tra le misure giuridiche di liceità, trova luogo anche del Regolamento comunale sulla videosorveglianza adottato dal Comune, in quanto disciplina il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza attivati nel territorio comunale (in particolare, individuando gli impianti di videosorveglianza di proprietà del Comune o da esso gestiti, definendo le caratteristiche e le modalità di utilizzo degli impianti di videosorveglianza e disciplinando gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti). All'interno del Regolamento comunale, infatti, sono disciplinate le procedure volte ad individuare ed autorizzare il personale che dovrà eseguire i trattamenti, le modalità di accesso ai locali ove sono posizionati i monitor di controllo ed i server posti a servizio dei sistemi di videosorveglianza, nonché le modalità di accesso degli interessati ai propri dati personali. Il personale della Polizia Locale autorizzato riceverà atto formale di individuazione con annesse istruzioni impartite e specifica formazione sulla tematica della videosorveglianza.
Si è proceduto, altresì, a siglare il patto per la sicurezza urbana, tra il Comune di NEVIANO e la Prefettura territorialmente competente in relazione all'impiego del sistema di videosorveglianza comunale.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile.

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

Il dato personale raccolto (immagine) è limitato allo stretto necessario ed in modo assolutamente pertinente alla finalità per cui è trattato, assicurando il pieno rispetto del principio di minimizzazione dei dati. L'attività di videosorveglianza è configurata, già in origine, limitando l'utilizzo di dati personali e di dati identificativi al minimo indispensabile, in modo da escluderne il trattamento quando non è strettamente necessario; in particolare quando le finalità possono essere perseguite mediante dati anonimi o limitando l'identificazione dei soggetti ai soli casi di necessità.

L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità sopra indicate, 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.
I dati vengono raccolti, infatti, 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. Il trattamento dei dati acquisiti mediante i sistemi di videosorveglianza in uso al Comune di NEVIANO, pertanto, avviene per le finalità che sono espressamente manifestate nelle informative, nel Regolamento comunale e in tutti gli altri atti e documenti in cui verranno successivamente rappresentate e ciò in ossequio all'art. 5, par. 1, lett. b), del Regolamento UE 2016/679. Per tale motivo, sono trattati solo ed esclusivamente i dati personali necessari e sufficienti per il raggiungimento delle finalità alla base del trattamento così come previsto dall'art. 5, par. 1, lett. c) del predetto Regolamento europeo.
Le procedure per accesso alle immagini registrate sono rigorose e possono essere attivate solo:

- sulla base di denunce di atti criminosi da parte dei cittadini;
- sulla base di segnalazioni relative ad atti criminosi pervenute agli Organi di Polizia;
- a seguito di atti criminosi che vengono rilevati direttamente dagli operatori di polizia nel visionare le immagini trasmesse in diretta dalle telecamere o nell'esercizio delle proprie funzioni;
- per attività di indagine;
- per motivi di sicurezza urbana (decreto del Ministero dell'Interno 5 agosto 2008).

In ogni caso, viene e verrà rispettato il PRINCIPIO DELLA MINIMIZZAZIONE DEI DATI (ovvero riducendo al minimo i dati, trattando solo quelli indispensabili per perseguire le finalità), anche perché non risulta possibile (ovvero si rivela non efficace) il ricorso a strumenti e sistemi di controllo alternativi; dove possibile i dati saranno anonimizzati (ovvero non più associabili all'interessato al quale si riferivano) o pseudonimizzati (ovvero renderli non immediatamente riconducibili al soggetto interessato senza ulteriori informazioni) e comunque cancellati al decorso del termine previsto (entro 7 giorni).

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

I dati sono esatti e aggiornati?

I dati trattati sono esatti e, ove necessario, il Titolare procederà ad eventuale rivisitazione ed aggiornamento, anche in base ai principi sopra elencati.
Per quanto riguarda le telecamere dotate di funzionalità di lettura targhe, il Comune ha valutato con attenzione la conformità delle funzionalità in questione con il principio di "esattezza" (art. 5, par. 1, lett. e), del Regolamento), anche in considerazione del fatto che, per quanto dichiarato dall'Autorità

Garante per la protezione dei dati personali in relazione all'utilizzo di tali strumenti, ad oggi i sistemi di videosorveglianza dotati di funzionalità di lettura automatizzata dei numeri di targa (OCR), per l'accertamento di illeciti di natura amministrativa, non risultano omologati da parte del Ministero delle Infrastrutture e dei Trasporti (cfr., in particolare, art. 45, comma 6, del Codice della strada e art. 192 del D.P.R. 445/1992). Per tale motivo, poiché per il perseguimento di tali finalità amministrative, non risulta, comunque, lecita la conservazione di informazioni relative a transiti di veicoli rispetto ai quali non siano stati rilevati - mediante consultazione automatizzata e in tempo reale di banche dati normalmente accessibili da parte della polizia locale in base alla disciplina di settore - illeciti di natura amministrativa (v. sent. TAR Veneto, sez. I, 4 gennaio 2022, n. 8), i dati raccolti tramite tali sistemi non vengono utilizzati per questa specifica finalità e sono cancellati entro il termine di 7 giorni (come sotto specificato).

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Qual è il periodo di conservazione dei dati?

I dati sono conservati per una durata massima di 7 giorni, con successiva cancellazione automatica, fatta eccezione per richieste da parte dell'Autorità giudiziaria o Forze di Polizia (in questi casi, può essere disposta la proroga del predetto termine di conservazione). Il server, pertanto, è stato dimensionato per poter contenere l'intera mole di dati per il periodo sopra indicato. La previsione del termine di giorni 7 (sette) per la conservazione dei dati raccolti, è stata determinata sulla base dei criteri di necessità, proporzionalità, pertinenza e non eccedenza ed anche sulle modalità indicate dall'Autorità Garante per la protezione dei dati personali nel provvedimento generale dell'8 aprile 2010 (paragrafo 3.4.3). 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

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Come sono informati del trattamento gli interessati?

Nelle zone in cui sono posizionate le telecamere è affissa adeguata segnaletica permanente (cartelli informativi) muniti di pittogramma e recanti la dicitura prevista dallo schema allegato al Provvedimento Generale del Garante per la protezione dei dati personali del 08.04.2010 e dalle recenti Linee guida dell'EDPB 3/2019 sul trattamento dei dati personali attraverso dispositivi video (adottate il 29 gennaio 2020). Infatti, risultano affissi dei cartelli recanti un'informativa in linea con le novità introdotte dal Reg. 679/16 e delle Linee guida n. 3/2019 EDPB e conformi alle indicazioni delle Autorità Garanti. Si specifica, inoltre, che nella sezione "privacy" del sito web istituzionale del Comune di NEVIANO, oltre all'informativa generale, viene riportata anche l'informativa completa sul trattamento dei dati di videosorveglianza ai sensi dell'art. 13 del Reg. UE 2016/679. Tale informativa 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.

In ogni informativa succinta contenente i dati essenziali, infatti, vi è il rinvio al sito del Comune di NEVIANO (ove trovare le informazioni complete). Il Comune di NEVIANO provvede con apposita campagna di informazione e sensibilizzazione rivolta alla cittadinanza per renderla edotta e consapevole della presenza e del funzionamento dei sistemi di videosorveglianza adottati in uso, nonché dei propri diritti all'opposizione, all'accesso, alla rettifica nonché tutti gli altri così come previsti dal regolamento europeo.

Riepilogando, pertanto, gli interessati sono informati mediante informative ad hoc (ex artt. 13 e 14 del GDPR) disponibili:

- NELLA SEZIONE "PRIVACY" SUL SITO ISTITUZIONALE VIENE RESA DISPONIBILE L'INFORMATIVA ESTESA
- IDONEA CARTELLONISTICA CHE SEGNALA LA PRESENZA DI SISTEMI DI VIDEOSORVEGLIANZA, BEN VISIBILE E PRIMA DEL RAGGIO DI AZIONE.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Ove applicabile: come si ottiene il consenso degli interessati?

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.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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

L'interessato, dietro presentazione di apposita istanza, ha diritto:

a) di ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;
b) di essere informato sugli estremi identificativi del titolare, del responsabile del trattamento, del responsabile della protezione dei dati, oltre che, sulle finalità e le modalità del trattamento dei dati;
c) di ottenere, senza ritardo e comunque non oltre 30 giorni dalla data di ricezione della richiesta:
    1. la conferma dell'esistenza o meno di dati personali che lo riguardano;
    2. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
    3. di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Il diritto di portabilità dei dati non è esercitabile stante l'inapplicabilità dell'art. 20 Reg. 201616791UE al trattamento oggetto di valutazione.

Nell'esercizio di tali diritti, l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia. Nel caso di esito negativo alle istanze, 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.

Tali diritti sono esercitabili scrivendo ai recapiti di contatto del Titolare del trattamento (Comune di Neviano) e/o del Responsabile della Protezione dei Dati dell'Ente, così come riportati nella cartellonistica e nell'informativa estesa.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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

Non è in concreto esercitabile, in riferimento alle immagini registrate, il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato si oppone al trattamento; i dati personali sono stati trattati illecitamente; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento.

Tale ultimo diritto è esercitabili scrivendo ai recapiti di contatto del Titolare del trattamento (Comune di Neviano) e/o del Responsabile della Protezione dei Dati dell'Ente, così come riportati nella cartellonistica e nell'informativa estesa.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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

Gli interessati possono esercitare i loro diritti di limitazione e di opposizione al trattamento contattando il Titolare del trattamento (Comune di Neviano) e/o del Responsabile della Protezione dei Dati dell'Ente.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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

Gli obblighi del Responsabile del trattamento sono assunti mediante specifico atto di nomina di responsabile del trattamento, ai sensi dell'art 28 del Reg U.E 2016/679.

Il Fornitore del servizio di implementazione e manutenzione degli impianti di videosorveglianza, opera, ai sensi dell'art. 28 del Regolamento, quale responsabile del trattamento dei dati personali per le attività collegate con l'esecuzione del Contratto, tramite interventi on-site e/o da remoto per il servizio di assistenza e manutenzione preventiva, correttiva ed evolutiva straordinaria relativa al sistema di videosorveglianza esistente, provvedendo a tutte le attività di manutenzione, riparazione e configurazione degli apparati, degli accessori e dei software per mantenerli in piena efficienza e funzionalità.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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

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

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni.

RISCHI

Misure esistenti o pianificate

Crittografia

Tutte le telecamere installate sono dotate di cifratura della trasmissione e, laddove stiano registrando su supporti interni, anche la registrazione è cifrata. Questo impedisce sia attacchi di tipo man-in-the-middle che la possibilità di accedere al registrato in seguito a sottrazione fisica del supporto.
Pertanto, la cifratura è garantita in tutte le fasi di trattamento dei dati video. Tuttavia, la registrazione all'interno del server di centralizzazione video non è invece cifrata, pur essendo protetta da password ed accessibile solo previa immissione di credenziali valide e autorizzate. La protezione fisica della registrazione centralizzata e dei relativi supporti è demandata alle misure di sicurezza della sala server.

Valutazione: Accettabile

Commento di valutazione: l'utilizzo della crittografia forte costituisce una misura di sicurezza adeguata a contrastare i rischi sulla riservatezza.

Anonimizzazione

I dati non possono essere anonimizzati, ma il tempo di conservazione delle immagini registrare non supera i sette (7) giorni dalla raccolta, in base a procedure di cancellazione automatica una volta decorso tale periodo di tempo. E' disponibile la funzione di privacy mask la quale può essere gestita sia dalle stesse telecamere che dal VMS. Il mascheramento può essere rimovibile in fase di esportazione del video se il livello utente lo consente.

Valutazione: Accettabile

Commento di valutazione: Misura non applicabile o applicabile in parte.

Controllo degli accessi logici

Solo i preposti possono accedere alle immagini in diretta ed alle immagini conservate sul server; attraverso dei propri username e delle proprie password.
Per l'accesso ai PC che gestiscono i sistemi di videosorveglianza, infatti, ci si avvale di un metodo di identificazione individuale, in quanto sono stati attuati metodi e mezzi di autenticazione e autorizzazione degli utenti abilitati all'accesso ai dati (tra cui, ad esempio, la lunghezza delle password e la frequenza della loro modifica). Ogni singolo utente è completamente profilabile, compresa l'assegnazione dettagliata di privilegi personali quali accesso, visualizzazione immagini, estrazione registrazioni.
Sono stati definiti anticipatamente i profili autorizzativi rispetto all'avvio delle attività di trattamento, si procede al controllo periodico sulla sussistenza delle condizioni per la conservazione dei profili autorizzativi e si adottano procedure per la gestione del ciclo di vita delle credenziali. Il VMS permette di definire i livelli autorizzativi per utenti e ruoli, prevedendo la possibilità di cambio della password da parte dell'utente. La scadenza della password è gestita manualmente dall'amministratore di sistema tramite l'opzione "Forza cambio password dell'utente all'accesso successivo.
In presenza di differenti competenze specificatamente attribuite ai singoli operatori si possono configurare diversi livelli di visibilità e trattamento delle immagini
Si procede alla disattivazione delle credenziali dell'autorizzato al trattamento nel caso in cui non sia più sussistente il presupposto o l'esigenza sottesa al rilascio delle credenziali stesse. L'operazione di disattivazione delle credenziali avviene selezionando lo stato "Disabilitato" relativo al profilo utente (in caso ad es. di assenza temporanea) oppure eliminandolo definitivamente. L'operazione è effettuabile esclusivamente dall'amministratore di sistema.

Si possono utilizzare differenti profili associati alle diverse utenze e adottare utenze nominali con revisione delle stesse da parte dei relativi possessori.
Per l'accesso alle immagini vi è l'obbligo di adozione di password alfanumerica pari a non meno di 8 caratteri alfanumerici e carattere speciale.

Valutazione: Accettabile

Commento di valutazione: Misura adeguata a contrastare i rischi previsti. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Tracciabilità applicata ai dati

Ogni operazione svolta dagli utenti viene tracciata e registrata. Il limite di conservazione dei log è di 365 giorni (spazio di archiviazione permettendo). Vengono impiegate e rispettate le ordinarie politiche di sicurezza e misure di prevenzione, al fine di ridurre la vulnerabilità del sistema di videosorveglianza poiché vi è un controllo periodico di tutti i LOG e degli Accessi, per verificare ex post l'effettiva necessità dell'accesso da parte delle persone designate/autorizzate (compreso la durata dei log).

Valutazione: Accettabile

Commento di valutazione: Misura adeguata a contrastare i rischi previsti (è presente un sistema di registrazione degli accessi logici e di tracciabilità applicata ai dati e/o sui sistemi: si tratta di un sistema di registrazione dei log degli accessi con possibilità di risalire agli stessi. La durata dei LOG non è inferiore a 6 mesi; comprendere se l'ingresso del manutentore viene registrato). Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Archiviazione

L'archiviazione sul server è fissata secondo i termini di conservazione dei dati come sopra indicato specificamente. Il tempo di mantenimento delle immagini e registrazioni è di 7 (sette) giorni e successivamente i dati sono sovrascritti automaticamente. Il VMS prevede la possibilità di impostare il tempo massimo di conservazione degli archivi video.
I dati vengono archiviati sui sistemi nell'esclusiva disponibilità del Comando di Polizia Locale, con tutte le misure di sicurezza applicate dalla società esterna che si occupa della manutenzione.

Valutazione: Accettabile

Commento di valutazione: Misura adeguata a contrastare i rischi previsti.

Minimizzazione dei dati

Sono raccolte le sole immagini di contesto, senza estrapolazione di dati biometrici o di altre categorie particolari di dati. Sono letti in automatico solo i dati relativi alle targhe dei veicoli che transitano sotto alcune specifiche telecamere dedicate, ma non vengono utilizzati per contestare sanzioni amministrative.
I dati sono trattati nel rispetto del principio di pertinenza e per le finalità per cui sono raccolti (es. solo per utilizzo P.G., ordine e sicurezza pubblica, prevenzione di reati, etc.).
L'accesso ai dati ripresi dalle telecamere e i risultati delle analisi effettuate dal sistema sulle registrazioni sono sottoposti a una limitazione di accesso da parte del solo personale della Polizia Locale opportunamente formato e addestrato sull'utilizzo del sistema e sulle regole della privacy.
Il posizionamento dei monitor è regolato in modo tale che solo il personale autorizzato possa accedere alla visualizzazione delle immagini.
I dati vengono periodicamente cancellati per evitare la loro accumulazione (sono state predisposte misure tecniche od organizzative per la cancellazione in forma automatica delle registrazioni, allo

scadere del termine previsto), le registrazioni hanno una durata massima di 7 giorni e la cancellazione è ciclica.
Nella realizzazione del sistema di videosorveglianza e nel montaggio delle telecamere sono state adoperate le logiche di Privacy by Design e Privacy by Default non prevedendo il trattamento di dati in numero superiore a quanto strettamente necessario per il perseguimento delle finalità previste (sono state predisposte misure tecniche od organizzative per la cancellazione in forma automatica delle registrazioni, allo scadere del termine previsto) e la dislocazione rispetta la riservatezza dei cittadini (es. domicili privati). In particolare, l'angolo visuale delle apparecchiature di ripresa è stato circoscritto alle aree o luoghi più esposti a pericoli, permettendo l'inquadratura solo delle zone funzionali al perseguimento delle finalità indicate e delle aree pubbliche a maggior rischio (con esclusione delle zone o aree non direttamente funzionali rispetto alle esigenze di sicurezza del sistema installato.
Il sistema di videosorveglianza, infine, garantisce:

- Limitazione della durata della conservazione (7 giorni);
- Limitazione all'accesso alle immagini in tempo reale (che avviene solo in base a effettive necessità);
- Possibilità di risalire ai log degli accessi al sistema di videosorveglianza per verificare ex post l'effettiva necessità dell'accesso da parte delle persone designate/autorizzate (compreso la durata dei log);
- Raccolta e conservazione delle informazioni solo in presenza di reati o eventi che abbiano minacciato la sicurezza;
- il mascheramento o l'offuscamento delle zone irrilevanti per la sorveglianza (è disponibile la funzione di privacy mask la quale può essere gestita sia dalle stesse telecamere che dal VMS. Il mascheramento può essere rimovibile in fase di esportazione del video se il livello utente lo consente);
- Trasparenza nei confronti degli interessati (mediante specifica "Informativa" sulla videosorveglianza da pubblicarsi sul sito web del Comune e tramite cartellonistica esposta nelle aree videosorvegliate);
- Le immagini vengono acquisite e registrate continuamente. L'accesso a tali immagini è però regolato da livelli di sicurezza che ne consentono la consultazione esclusivamente a personale e/o utenti autorizzati in tal senso.

Valutazione: Accettabile

Commento di valutazione: si potrebbe implementare una misura che consenta di effettuare l'editing di immagini di terzi, quando si forniscono filmati agli interessati. Tuttavia, il formato di esportazione del VMS non prevede modifica, ed in caso di manipolazione questo viene segnalato. Inoltre, il contenuto video esportato può essere protetto da una password che diventa anche chiave di cifratura del contenuto stesso.

Vulnerabilità

Al fine di ridurre la vulnerabilità del sistema di videosorveglianza, il server risulta connesso ad un rete internet dedicata protetta da firewall. Vengono impiegate e rispettate le ordinarie politiche di sicurezza e misure di prevenzione, al fine di ridurre la vulnerabilità del sistema di videosorveglianza. I software e l'hardware sono aggiornati al bisogno e periodicamente (patch e aggiornamenti strutturali) durante l'attività di manutenzione compiuta dal Responsabile del trattamento dei dati.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Lotta contro il malware

Il sistema non invia e/o riceve dati dall'esterno. Il collegamento esterno avviene solo per aggiornamenti del S.O.

Antivirus su server e client del sistema di videosorveglianza: sul server e sui client è presente un antivirus che previene eventuali attacchi esterni o la ricezione di software dannosi.

Sono state implementate soluzioni basate su hardware e software quali firewall.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Gestione postazioni

L'accesso fisico alle postazioni di visualizzazione e all'area in cui è ubicato il server/NVR di videosorveglianza è limitato al solo personale autorizzato e appositamente istruito, in locali a ciò appositamente adibiti. Il PC, sito nell'ufficio della sala di controllo che necessita di apposita chiave per l'accesso, è utilizzabile solo dal preposto o dai preposti muniti di credenziali di accesso personali.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Manutenzione

In caso di interventi derivanti da esigenze di manutenzione, i soggetti preposti sono costituti da soggetti interni o esterni che possono accedere alle immagini (solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche). Gli interventi di manutenzione vengono effettuati da personale tecnicamente qualificato per intervenire sul sistema. E' possibile però che un soggetto interno abbia in custodia le password per accedere alla gestione del sistema.

Il Responsabile del trattamento provvede, secondo quanto stabilito da contratto, alla manutenzione programmata. L'attività è condotta in locale e/o in outsourcing, mediante collegamento agli strumenti in uso.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Contratto con il responsabile del trattamento

E' stato sottoscritto l'atto di designazione a Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (EU) n. 679/2016 con la società fornitrice del servizio di installazione e manutenzione del sistema di videosorveglianza comunale, cui si rimanda, contenente altresì specifiche istruzioni da conferire al personale dipendente che può avere accesso alle immagini.

I dati personali comunicati e gestiti dal responsabile del trattamento beneficiano di garanzie sufficienti (in particolare, quanto a conoscenze specialistiche, affidabilità e risorse) e sono state comunicate le misure di sicurezza che detto sistema garantisce.
Il fornitore garantisce un'assistenza continua e, in qualità di responsabile del trattamento, garantisce anche tutte le misure di sicurezza tecniche e organizzative, compreso il rispetto dei principi di privacy by design e privacy by default, nel rispetto della vigente normativa (D. Lgs. n. 196/2003 e s.m.i. nonché il Regolamento Ue 2016/679).

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Sicurezza dei canali informatici

Protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione. La trasmissione di comunicazioni di immagini riprese viene effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza (la protezione della trasmissione dei filmati è assicurata attraverso canali di comunicazione sicuri a prova di intercettazione).
Il sistema di videosorveglianza normalmente si connette alla rete internet manualmente ad opera del personale della Polizia Locale, solo per attività di aggiornamento software o per attività di manutenzione in remoto su canale VPN.
Tutti gli apparati di ripresa digitali connessi a reti informatiche, pertanto, sono protetti contro i rischi di accesso abusivo di cui all´art. 615-ter del codice penale.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Controllo degli accessi fisici

Il computer da cui si accede al server è collocato in un apposito locale chiuso a chiave, accessibile solo al designato al trattamento, ai preposti, a tecnici della manutenzione designati dal responsabile del trattamento, tutti ritualmente nominati. Vi è, quindi, la garanzia che tutti i locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in cui vengono conservate le riprese video siano protetti contro l'accesso non supervisionato da parte di terzi.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Tracciabilità sui sistemi

Ogni accesso al sistema è registrato in un apposito log (registrazione e la revisione periodica delle azioni eseguite dagli utenti, con riguardo sia al sistema sia ai dati) ed è compito del Comandante della Polizia Locale effettuare revisioni mensili di queste informazioni per accertarsi del regolare utilizzo dei dati e prevenire in tal modo ogni abuso.

Valutazione: Accettabile

Commento di valutazione: sono registrati i LOG di ogni operazione, da intendersi la mera registrazione e la revisione periodica delle azioni eseguite dagli utenti, con riguardo sia al sistema sia ai dati.

Prevenzione delle fonti di rischio (anche non umane)

L'ubicazione dei supporti sui quali vengono registrati i dati è in locali climaticamente controllati da sistema di riscaldamento e raffrescamento e protetti da infiltrazioni di acqua o di condensa. I quadri elettrici di alimentazione sono dotati di scaricatore di sovratensione per evitare che eventi elettrici possano arrecare danno alle apparecchiature. È presente un UPS per garantire continuità di servizio in caso di interruzione dell'erogazione di corrente e protezione intrinseca (filtro bassa basso) da sbalzi di tensione o corrente.

Valutazione: Accettabile

Commento di valutazione: si consiglia un aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Politica di tutela della privacy

Adeguamento continuo dell'Ente a quanto previsto dal GDPR, tra cui la nomina del DPO e il costante coinvolgimento dello stesso.
All'interno del Comune esiste un'organizzazione idonea a guidare e verificare la protezione dei dati personali all'interno dell'Ente (designazione di un DPO/RPD, creazione di un gruppo di lavoro interno, presenza di designati ex art. 2-quaterdecies D.Lgs. 196/2003, etc.).
Il titolare del trattamento è dotato di una struttura tecnica-organizzativa in grado di mappare i processi inerenti il trattamento dei dati e di redigere le valutazioni di impatto nei casi previsti, porre in essere le misure di sicurezza per minimizzare i rischi di violazione, documentare le violazione dei dati personali, fornire supporto al fine di superarle o minimizzare il danno e, nei casi previsti, notificarle al Garante e comunicarle agli interessati e cooperare con l'autorità di controllo quando richiesto.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento. Per quanto riguarda il trattamento, il Modello di Gestione sulla Protezione dei dati è in fase di predisposizione/aggiornamento e si sostanzierà in una serie di procedure interne (es. Regolamento per l'utilizzo degli strumenti informatici, posta elettronica e Internet, Procedura per l'esercizio dei diritti, Procedura per la gestione delle violazioni di dati personali, etc.).

Gestione delle politiche di tutela della privacy

Il Comune dispone di una base documentale che formalizza gli obiettivi e le regole da applicare nel campo della protezione dei dati (piano d'azione, revisione periodica delle politiche in materia di protezione dati, ecc.).
Sono state definite e applicate procedure per la concessione, la modifica e la revoca dell'accesso alle video riprese.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali.

Impostate corrette procedure di data breach e formazione dei soggetti autorizzati. Esiste una procedura interna e istruzioni operative per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni ecc.). Il fornitore responsabile del trattamento è obbligato contrattualmente a supportare il Titolare nella gestione di ogni violazione dei dati personali (data breach), al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32 - 34 del GDPR.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Gestione del personale

In presenza di differenti competenze, specificatamente attribuite ai singoli operatori, sono stati configurati diversi livelli di visibilità e trattamento delle immagini. I designati incaricati sono in possesso di credenziali di autenticazione che permettono di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza.
Nel caso di interventi derivanti da esigenze di manutenzione, i soggetti preposti sono costituti da soggetti interni che possono accedere alle immagini (solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche).
Per quanto riguarda il Comune e il Fornitore, entrambi assicurano al proprio personale e ai collaboratori:

- la corretta informazione sui loro ruoli e responsabilità nell'ambito della sicurezza delle informazioni prima di ottenere l'accesso a sistemi informativi riservati;
- la predisposizione di linee guida circa le norma comportamentali da tenere negli uffici relative all'ambito della sicurezza delle informazioni;
- il raggiungimento di un adeguato livello di consapevolezza in materia di sicurezza delle informazioni adatto ai loro ruoli e responsabilità all'interno dell'Amministrazione attraverso opportune campagne di sensibilizzazione e piani di formazione;
- l'adeguamento dei termini e delle condizioni del rapporto di lavoro;
- formazione periodica;

In tal senso, il Comune attua un programma di sensibilizzazione alla sicurezza delle informazioni e formazione sugli obblighi derivanti dal Reg. UE 2016/679, rendendo consapevoli personale e collaboratori delle loro responsabilità e degli strumenti con cui gestire queste responsabilità. Il Comune adotta varie tipologie di erogazione per sensibilizzare le proprie risorse, quali formazione in aula, formazione a distanza, web-based, auto-apprendimento e altre.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Istruzioni per la gestione degli strumenti

Il personale preposto al trattamento dei dati è stato formato sull'utilizzo degli strumenti software e hardware di cui si compone il sistema di videosorveglianza.

Sono state fornite, inoltre, istruzioni per evitare riprese particolareggiate nei casi in cui le stesse non siano indispensabili in relazione alle finalità perseguite.
Sono presenti specifiche lettere di autorizzazione e linee guida interne per il personale che può trattare tali dati ed è stata predisposta la lettera di Designato interno (ex art. 2-quaterdecies del D. Lgs. 196/2003) in capo al Comandante.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Gestione dei terzi che accedono ai dati

Esiste una procedura volta a ridurre i rischi per le libertà e la vita privata degli interessati potenzialmente conseguenti all'accesso legittimo ai dati da parte di terzi quali (quali Forze di Polizia, su mandato dell'Autorità Giudiziaria, Carabinieri, Guardia di Finanza, etc.), mediante identificazione di tali soggetti terzi, verifica di un altro presupposto di liceità per l'accesso ai dati o per la comunicazione di tali dati (es. invio delle richiesta via PEC o richiesta in loco presso il Comando, compilazione di uno specifico modulo con la richiesta di estrazione dati e consegna dati su supporto quale CD/DVD o chiavetta USB).

Valutazione: Accettabile

Commento di valutazione: Al momento il sistema è chiuso agli accessi di soggetti esterni al comando di PM. Se dovesse rendersi necessario predisporre una o più connessioni al servizio di altre forze di polizia, la scelta ricadrà su una VPN crittografata, la rete di trasporto sarà individuata e scelta tra le opzioni disponibili in funzione dello specifico collegamento (internet, WLAN, F.O. ecc). Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Trasparenza nei confronti dell'interessato

Appositi cartelli sono applicati in prossimità a ogni area videosorvegliata, al fine di informare della presenza di un sistema di videosorveglianza. Esiste una informativa sul trattamento dei dati, che viene messa a disposizione di ogni interessato al trattamento coinvolto nella rilevazione e registrazione delle immagini (ciò avviene mediante apposita cartellonistica, che rinvia a una informativa più completa presente sul sito web del Comune). L'esistenza delle telecamere, infatti, viene opportunamente evidenziata in ogni area interessata.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Metodo adottato per l'analisi dei rischi.

Il modello scelto per quantificare i rischi è quello della misurazione dell'esposizione al rischio:

Esposizione = probabilità x danno

La valutazione del rischio è data dalla combinazione di due parametri, ai quali si attribuisce un valore numerico a seconda della loro valutazione qualitativa. Al fine di oggettivare tale valutazione, si è adottata la metrica proposta da ENISA nel documento "Handbook on Security of Personal Data Processing":

- **gravità del rischio**, intesa come possibile effetto sulla dignità e libertà degli interessati oppure danni materiali agli stessi derivanti dal verificarsi dell'evento considerato a rischio (la gravità del rischio può essere Bassa [1], Media [2], Alta [3], Significativa [4]). I 4 livelli di impatto si possono così descrivere:
    - Bassa [1]: Le persone possono incontrare alcuni piccoli inconvenienti, che supereranno senza problemi (tempo speso per reinserire le informazioni, fastidi, irritazioni, ecc.).
    - Media [2]: Gli individui possono incontrare notevoli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà (costi extra, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
    - Alta [3]: Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera da parte di istituzioni finanziarie, danni alla proprietà, perdita del lavoro, mandato di comparizione, peggioramento della salute, ecc.).
    - Significativa [4]: Gli Individui possono subire conseguenze significative o addirittura irreversibili, che potrebbero non superare (incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.).
- **probabilità di accadimento** della minaccia rilevata, sulla base della natura delle minacce, delle fonti di rischio e delle misure esistenti o pianificate (la probabilità può essere Improbabile [1], Bassa [2], Media [3], Alta [4]). I 4 livelli di probabilità di accadimento si possono così descrivere:
    - Improbabile [1]: Appare impossibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
    - Bassa [2]: Appare difficile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
    - Media [3]: Appare possibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
    - Alta [4]: Appare estremamente probabile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
- **vulnerabilità** rispetto al grado di adeguatezza delle misure (Vu): grado di adeguatezza delle misure che contrastano il manifestarsi degli eventi.

Viene pertanto identificata l'esposizione al rischio, intesa come combinazione moltiplicativa dei due fattori, da cui vengono stabilite le azioni da compiere sulla base della seguente tabella:

Probabilità	Alta	4	4	8	12	16
	Media	3	3	6	9	12
	Bassa	2	2	4	6	8
	Improbabile	1	1	2	3	4
			1	2	3	4
			Bassa	Media	Alta	Significativa
			Gravità			

La tabella su indicata tiene presente, quindi, il rischio finale calcolato in funzione dei 3 fattori seguenti: RN = f (P, G, Vu)

Le azioni consequenziali da intraprendere sono le seguenti:

Livello di esposizione	**Intervallo di valori**	**Intervento previsto**
Minimo	1-3	Da Monitorare
Medio	4-8	Implementare le misure previste entro l'anno
Significativo	9-16	Intervento urgente

ACCESSO ILLEGITTIMO AI DATI (PERDITA DI RISERVATEZZA)

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

- Lesione dei diritti fondamentali degli interessati (es. lesione del diritto d'immagine, percezione di insicurezza)
- Danno da trattamento illecito/non corretto
- Divulgazione illecita di dati personali
- Effetti invasivi sulla sfera di autodeterminazione delle persone riprese
- Conoscenza di dati da parte di terzi non autorizzati (es. lesione del diritto alla riservatezza)
- Perdita della libertà o della libertà di movimento
- Coinvolgimento dei dati personali in un modo che vada oltre le ragionevoli aspettative delle persone fisiche
- Sensazione di sistematico monitoraggio
- Intromissione inaccettabile nella vita privata o nella vita pubblica
- Impedimento dell'esercizio del controllo sui dati personali o limitazione dei diritti

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- attacchi informatici o attacco da remoto ai sistemi da parte di hacker
- accesso non autorizzati alla sala di controllo
- visione dei monitor in diretta per una finalità illegittima, se non illecita
- abusi di privilegi di accesso o utilizzo improprio da parte del personale autorizzato all'accesso/visione delle immagini
- errori nei processi di elaborazione
- perdita dati per guasto/furto/smarrimento hardware (es. perdita dei dati dovuti al furto del DVR, server o delle schede dove sono memorizzate le immagini degli interessati)
- inefficiente gestione del dato
- raccolta ingiustificata o eccessiva di dati
- uso improprio o abuso dei dati (es. uso dei dati oltre le ragionevoli aspettative degli individui, l'uso insolito di dati oltre le norme dell'Amministrazione)
- perdita o furto o distruzione e alterazione dei dati
- accesso illegittimo al sistema informativo e ai dati (perdita di confidenzialità)
- accesso abusivo al server o accesso abusivo presso il Comando
- comportamento illecito/illegittimo degli utenti, operatori o amministratori di sistema
- accesso non autorizzato o accesso improprio degli autorizzati
- controllo e monitoraggio eccessivo (derivante dal monitoraggio sistematico delle aree accessibili al pubblico)
- furto degli hardware dell'impianto
- obsolescenza e/o mancato aggiornamento dei dispositivi
- raccolta ingiustificata o eccessiva di dati
- intercettazione
- attacchi al sistema di autenticazione o variazione non autorizzata delle credenziali di accesso al sistema informativo
- mancanza di trasparenza nei confronti degli interessati
- malware

Quali sono le fonti di rischio?

- Fonti umane interne: dipendenti che compiono azioni involontarie o fraudolente per motivi di confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio.
- Fonti umane esterne:

1) un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo;
2) un attaccante che prende di mira la società esterna incaricata della manutenzione;
3) una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni.

Le motivazioni possono essere molteplici: dallo scherzo alla molestia, alla mera curiosità dell'operatore autorizzato, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.
Fonti non umane: un incidente o un sinistro (interruzioni di corrente, incendio, inondazione, ecc.).

Per tali motivi, si ritiene molto più probabile che i pericoli per i diritti e le libertà delle persone fisiche

- che impattano sui vari sistemi di videosorveglianza utilizzati
- possano derivare da aspetti tecnici e organizzativi propri del titolare del trattamento e si identificano in strumenti, persone e procedure o attività che sono parte integrante del trattamento in questione o sono ad esso correlati. Si tratta, quindi di personale interno ed esterno malintenzionato oppure accesso tramite internet o accesso abusivo fisicamente all'interno del Comando.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità applicata ai dati, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Tracciabilità sui sistemi, Prevenzione delle fonti di rischio, Protezione contro fonti di rischio (anche non umane), Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Istruzioni per la gestione degli strumenti, Gestione dei terzi che accedono ai dati, Trasparenza nei confronti dell'interessato.

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

ALTA: I DATI TRATTATI SONO RILEVANTI, ANCHE SE I MECCANISMI DI CANCELLAZIONE AUTOMATICA NEL BREVE PERIODO E LE MISURE DI PROTEZIONE ADOTTATE RENDONO LA GRAVITA' DEL RISCHIO NON MASSIMA.
Gli interessati potrebbero sperimentare inconvenienti significativi, ma superabili. La gravità delle conseguenze di un ipotetico accesso non autorizzato agli impianti di videosorveglianza sono del tutto trascurabili. Chi accede agli impianti può visionare unicamente immagini riguardanti persone e cose presenti in un pubblico spazio (territorio urbano) o, in alcuni casi, il transito di un determinato veicolo, in precise circostanze di tempo e di luogo. Non essendoci impianti con caratteristiche di riconoscimento biometrico, è impossibile associare univocamente una figura umana che compare nelle immagini ad una persona fisica. E' invece possibile, in via ipotetica, riscontrare passaggi di veicoli attraverso una ricerca mirata per targa.

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

BASSA: LE MISURE DI PROTEZIONE ADOTTATE, NONCHE' LA CONSAPEVOLEZZA DEGLI AUTORIZZATI, RENDONO LA PROBABILITA' DEL RISCHIO NON ELEVATA.
Appare non molto probabile che le fonti di rischio considerate concretizzino una minaccia. Le misure di sicurezza appaiono adeguate a proteggere i dati personali trattati da accessi non autorizzati in considerazione del contesto degli impianti che sono in funzione. La probabilità di concretizzazione del rischio di accesso illegittimo ai dati è trascurabile, soprattutto per quanto concerne gli attacchi di

soggetti esterni all'ente. Il server, per la parte della videosorveglianza non è collegato ad internet (riducendo drasticamente, quindi, la già scarsissima probabilità di attacco informatico esterno).

Livello di esposizione al rischio

GRAVITA'	PROBABILITA'	ESPOSIZIONE	INTERVENTO PREVISTO
3	2	6	Nessun intervento previsto. Le misure di sicurezza individuate e applicate consentono una riduzione importante del rischio finale

Valutazione: Accettabile

Commento di valutazione: in caso di accesso illegittimo alle immagini si ritiene non si concretizzi un danno elevato in capo all'interessato, in quanto il soggetto terzo non autorizzato prenderebbe semplicemente visione delle immagini registrate (di soggetti difficilmente identificabili in assenza di ulteriori informazioni). L'utilizzo delle immagini, in ogni caso, avviene in maniera conforme alle finalità dichiarate ai cittadini e il personale coinvolto (interno ed esterno) è informato sulle regole e modalità di trattamento da rispettare per non violare la normativa in materia di protezione dei dati. Le misure di sicurezza adottate prevengono in maniera abbastanza adeguata ogni rischio di accesso abusivo ai sistemi di videosorveglianza.

MODIFICHE INDESIDERATE DEI DATI

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

- Lesione dei diritti fondamentali degli interessati (es. lesione al diritto all'immagine, percezione di insicurezza);
- Lesione all'integrità del dato personale;
- Impossibilità di tutela a seguito di un reato subito;
- Danno da trattamento illecito/non corretto (danno economico o sociale);
- Impedimento dell'esercizio del controllo sui dati personali o limitazione dei diritti;
- Lesione del diritto a difendersi in giudizio civile o in un processo penale;
- Condotta di indagini giudiziarie nei confronti di persone sbagliate;

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

- accesso non autorizzati alla sala di controllo
- attacco da remoto ai sistemi da parte di hacker
- errata elaborazione dei dati
- attacchi informatici
- abusi di privilegi di accesso o utilizzo improprio
- errori nei processi di elaborazione
- inefficiente gestione del dato
- alterazione dei dati illecita o non autorizzata
- alterazione delle impostazioni di funzionamento del server o del DVR o delle telecamere
- accesso abusivo al server o accesso abusivo presso il Comando
- comportamento illecito/illegittimo degli utenti, operatori o amministratori di sistema
- accesso non autorizzato o accesso improprio degli autorizzati
- obsolescenza e/o mancato aggiornamento dei dispositivi
- attacchi al sistema di autenticazione o variazione non autorizzata delle credenziali di accesso al sistema informativo
- malware
- danneggiamento degli hardware o dei software dell'impianto
- uso o conservazione dei dati inesatti o non aggiornati

Quali sono le fonti di rischio?

- Fonti umane interne: dipendenti che compiono azioni involontarie o fraudolente per motivi di confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio.
- Fonti umane esterne: 1) un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo; 2) un attaccante che prende di mira la società esterna incaricata della manutenzione; 3) una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni e alterarle.
- Fonti non umane: un incidente o un sinistro (interruzioni di corrente, incendio, inondazione, ecc.).
- Per tali motivi, si ritiene che i pericoli per i diritti e le libertà delle persone fisiche – che impattano sui vari sistemi di videosorveglianza utilizzati – possano derivare da aspetti tecnici e organizzativi propri del titolare del trattamento e si identificano in strumenti, persone e procedure o attività che sono parte integrante del trattamento in questione o sono ad esso correlati. Si tratta, quindi di personale interno ed esterno malintenzionato oppure accesso tramite internet o accesso abusivo fisicamente all'interno del Comando. Non sono da escludere

nemmeno eventi calamitosi non imputabili al Titolare del trattamento (guasto, incendio o calamità naturali).

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

Controllo degli accessi logici, Tracciabilità applicata ai dati, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Tracciabilità sui sistemi, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Prevenzione delle fonti di rischio (anche non umane), Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Istruzioni per la gestione degli strumenti, Gestione dei terzi che accedono ai dati.

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

ALTA: IL RISCHIO DI MODIFICHE INDESIDERATE RIGUARDA PRINCIPALMENTE I TRATTAMENTI ERRATI DERIVANTI DA AZIONI UMANE CHE POTREBBERO PORTARE A CONSEGUENTI ELABORAZIONI ERRATE DEI DATI, DA ATTACCHI INFORMATICI O MALWARE OVVERO DA GUASTI HARDWARE O SOFTWARE.
Una modificazione indesiderata delle immagini comporterebbe un rischio con riguardo al profilo psicologico dell'interessato. Il senso di violazione della propria riservatezza sarebbe apprezzabile, sebbene priva di danni irreparabili. Ciò potrebbe comportare un disturbo di contenuta gravità ma oggettivo, soprattutto nelle persone più suscettibili. Le immagini alterate potrebbero essere utilizzate, in linea teorica, per schemi, intimidazioni o ricatti verso gli interessati ad opera di malintenzionati.

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

IMPROBABILE: LE MISURE ADOTTATE RENDONO LA PROBABILITA' DI RISCHIO MOLTO LIMITATA. Appare altresì difficile che si realizzi una modifica indesiderata dei dati in questione, considerando la tipologia di dati trattati (immagini e targhe veicoli).
Sebbene il rischio zero sia da considerarsi un'utopia a carattere precipuamente teorico, la modifica dell'immagine raccolta da una telecamera di videosorveglianza è un'operazione tecnicamente molto complessa. Il rapporto costi/benefici tra i mezzi impiegati ed i risultati ottenuti per compiere l'azione illecita risulta davvero sproporzionato (es. sistemi di intelligenza artificiale in grado di modificare le immagini).
In ogni caso, le misure di sicurezza che sono state adottate contribuiscono ad abbattere drasticamente la già scarsissima probabilità di verificazione dell'evento.

Livello di esposizione al rischio

GRAVITA'	PROBABILITA'	ESPOSIZIONE	INTERVENTO PREVISTO
3	1	3	Nessun intervento previsto. Le misure di sicurezza individuate e applicate consentono una riduzione importante del rischio finale

Valutazione: Accettabile

Commento di valutazione: per poter modificare i video le persone che si volessero cimentare dovrebbero possedere una tecnologia molto avanzata; appare, pertanto, molto improbabile che i rischi individuati possano realizzarsi.

PERDITA DI DATI

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

- Lesione dei diritti fondamentali degli interessati
- Lesione alla integrità del dato personale
- Percezione di insicurezza
- Impossibilità di tutela a seguito di un reato subito
- Danno da trattamento illecito/non corretto (danno economico o sociale)
- Impedimento dell'esercizio del controllo sui dati personali o limitazione dei diritti
- Lesione del diritto a difendersi in giudizio civile o in un processo penale.

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

- attacchi informatici da remoto al sistema
- accesso non autorizzati alla sala di controllo
- malfunzionamenti fisici dei sistemi
- cancellazione accidentale
- abusi di privilegi di accesso o utilizzo improprio
- errori nei processi di elaborazione
- perdita dati per guasto/furto/smarrimento hardware (es. perdita dei dati dovuti al furto del DVR, server o delle schede dove sono memorizzate le immagini degli interessati)
- inefficiente gestione del dato
- perdita, furto o distruzione dei dati
- accesso abusivo al server o accesso abusivo presso il Comando
- comportamento illecito/illegittimo degli utenti, operatori o amministratori di sistema
- furto degli hardware dell'impianto o delle schede dove sono memorizzate le immagini degli interessati
- obsolescenza e/o mancato aggiornamento dei dispositivi
- attacchi al sistema di autenticazione o variazione non autorizzata delle credenziali di accesso al sistema informativo
- malware
- danneggiamento degli hardware o dei software dell'impianto
- malfunzionamenti/Danni infrastrutturali,
- eventi meteorologici/naturali,
- atti vandalici/danneggiamento delle videocamere.
- cancellazione dei log e/o delle immagini

Quali sono le fonti di rischio?

- Fonti umane interne: dipendenti che compiono azioni involontarie o fraudolente per motivi di confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio.
- Fonti umane esterne: 1) un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo; 2) un attaccante che prende di mira la società esterna incaricata della manutenzione; 3) una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni e alterarle.
- Fonti non umane: un incidente o un sinistro (interruzioni di corrente, incendio, inondazione, ecc.).

Per tali motivi, si ritiene che i pericoli per i diritti e le libertà delle persone fisiche – che impattano sui vari sistemi di videosorveglianza utilizzati – possano derivare da aspetti tecnici e organizzativi propri

del titolare del trattamento e si identificano in strumenti, persone e procedure o attività che sono parte integrante del trattamento in questione o sono ad esso correlati. Si tratta, quindi di personale interno ed esterno malintenzionato oppure accesso tramite internet o accesso abusivo fisicamente all'interno del Comando. Non sono da escludere nemmeno eventi calamitosi non imputabili al Titolare del trattamento (*guasto, incendio, eventi metereologici o calamità naturali*).

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

Controllo degli accessi logici, Tracciabilità applicata ai dati, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Tracciabilità sui sistemi, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Prevenzione delle fonti di rischio (anche non umane), Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Istruzioni per la gestione degli strumenti, Gestione dei terzi che accedono ai dati.

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

MEDIA: LA GRAVITA' NON RISULTA DI LIVELLO ELEVATO, IN QUANTO LA MANCANZA DEI DATI NON CREA ALCUN RISCHIO PARTICOLARE IN CAPO AGLI INTERESSATI.
Una perdita indesiderata delle immagini comporterebbe un rischio limitato per l'interessato.

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

BASSA: LE MISURE DI PROTEZIONE ADOTTATE, NONCHE' LA CONSAPEVOLEZZA DEGLI AUTORIZZATI, RENDONO LA PROBABILITA' DEL RISCHIO NON ELEVATA.
Sebbene possa apparire possibile che le fonti di rischio considerate concretizzino una minaccia sulla base delle caratteristiche dei supporti (ad esempio: furto delle videocamere o atti di vandalismo a danno delle apparecchiature), le misure di sicurezza adottate rendono la probabilità di accadimento molto bassa.
Le misure di sicurezza che sono state adottate contribuiscono ad abbattere drasticamente la probabilità di verificazione di una perdita dei dati.

Livello di esposizione al rischio

GRAVITA'	PROBABILITA'	ESPOSIZIONE	INTERVENTO PREVISTO
2	2	4	Nessun intervento previsto. Le misure di sicurezza individuate e applicate consentono una riduzione importante del rischio finale

Valutazione: Accettabile

Commento di valutazione: appare non molto probabile che le fonti di rischio considerate concretizzino una minaccia e le misure di sicurezza adottate consentono di considerare "minimo" il livello di materializzazione del rischio. Le misure di sicurezza adottate prevengono in maniera abbastanza adeguata ogni rischio di accesso abusivo ai sistemi di videosorveglianza, fermo restando la necessità di continui aggiornamenti per mitigare ulteriormente il rischio.

PIANO D'AZIONE

Misure di prevenzione e protezione previste

La seguente tabella illustra, sulla base delle risultanze della valutazione dei rischi, le misure di prevenzione e protezione da attuare nel prossimo periodo.

Misura	Efficacia	Adottata	Programmata
Formazione	La formazione aumenta la consapevolezza e la cultura sulla materia affrontata. Conseguentemente si riduce il rischio correlato, in particolare, ai comportamenti dei soggetti attivi.	NO	Occorre programmare sessione formativa suppletiva per i designati e autorizzati interni sul tema videosorveglianza alla luce delle linee guida dell'EDPB.
Informativa	L'informativa aumenta la consapevolezza nei soggetti passivi e riduce il rischio di percepire il trattamento come un controllo dell'attività lavorativa e aumenta il livello di gradimento da parte dei soggetti passivi.	SI	Misura già adottata
Installazione a norma	L'installazione a norma permette di ridurre i rischi da interferenze esterne sia da parte di persone che dovuti a cause di forza maggiore o indipendenti da persone fisiche. Inoltre, permette di ridurre il rischio derivante da un trattamento eccessivo, sproporzionato o non necessario.	SI	Misura già adottata
Misure organizzative	La definizione di misure organizzative (per esempio policy, procedure, mansionari…) aumenta il grado di responsabilizzazione dei soggetti attivi e, combinata con la formazione, migliora la cultura in materia. Inoltre, garantisce e tutela maggiormente i diritti degli interessati e contribuiscono a definire sia una sistema di controllo che un sistema disciplinare.	SI	Misura già adottata
Misure tecniche ICT	Le misure tecniche ICT permettono di limitare il trattamento dei dati e di implementare le misure di protezione dei dati per impostazione predefinita. In particolare, l'impatto maggiore riguarda le caratteristiche relative all'accesso ai dati (sistema di autorizzazione, sistema di autenticazione), alla loro cancellazione automatica e alla loro conservazione.	SI	Misure già adottate, ma è necessario implementare la tracciabilità sui dati e sui sistemi

Principi fondamentali

SI	ACC	MIG	ELENCO PRINCIPI
X	X		Finalità
X	X		Basi legali
X	X		Adeguatezza dei dati
X	X		Esattezza dei dati
X	X		Periodo di conservazione
X	X		Informativa
n/a	-	-	Raccolta del consenso
X	X		Diritto di accesso e portabilità dei dati
X	X		Diritto di rettifica e diritto di cancellazione (ove compatibili il perseguimento delle finalità di pubblico interesse come previsto dall'art. 6 par. 1 lett. e), del GDPR)
X	X		Diritto di limitazione e diritto di opposizione (ove compatibili finalità di pubblico interesse come previsto dall'art. 6 par. 1 lett. e), del GDPR)
X	X		Responsabili del trattamento
X	X		Trasferimenti di dati

ACC: Principi valutati Accettabili
MIG: Principi valutati Migliorabili

Piano d'azione

Si ritiene che le misure tecniche ed organizzative adottate siano adeguate al rischio collegato all'attività di trattamento in esame.
Il Comando di Polizia Locale, nel rispetto dei patti per la sicurezza urbana e del Regolamento comunale, ha valutato la necessità di installare gli impianti di videosorveglianza al fine di soddisfare e garantire la tutela della sicurezza pubblica (mediante anche la valutazione di soluzioni alternative ma tutte difficilmente applicabili), individuando opportune garanzie per il rispetto della riservatezza e dignità dei cittadini.
Si ritiene, tuttavia, di effettuare con cadenza annuale o biennale attività di audit sui profili di autorizzazione del personale interno in possesso delle credenziali di accesso ai vari sistemi e sul responsabile del trattamento, allo scopo di verificare il rispetto dell'accordo sulla protezione dei dati personali.
Si ritiene necessario aggiornare la presente DPIA al verificarsi di una delle seguenti condizioni:

- modifica del sistema hardware e/o software in uso;
- implementazione di nuove tecnologie (ad es. di tipo intelligente o di riconoscimento biometrico tramite "Alert riconoscimento facciale", che consente la visualizzazione dei volti di una scena o la ricerca del volto in una scena in base a immagini in archivio o rilevate nel video);
- aggiornamenti normativi o chiarimenti interpretativi delle Autorità Garanti per la protezione dei dati personali;
- - variazione del soggetto operante in qualità autorizzato al trattamento o di responsabile del trattamento.

Misure esistenti e pianificate

SI	ACC	MIG	ELENCO MISURE
X	X		Crittografia
X	X		Anonimizzazione
X	X		Controllo degli accessi logici
X	X		Tracciabilità applicata ai dati
X	X		Archiviazione
X	X		Minimizzazione dei dati
X	X		Vulnerabilità
X	X		Lotta contro il malware
X	X		Gestione postazioni
X	X		Manutenzione
X	X		Contratto con il responsabile del trattamento
X	X		Sicurezza dei canali informatici
X	X		Controllo degli accessi fisici
X	X		Tracciabilità sui sistemi
X	X		Politica di tutela della privacy
X	X		Gestione delle politiche di tutela della privacy
X	X		Gestione delle postazioni
X	X		Prevenzione delle fonti di rischio (anche non umane)
X	X		Gestire gli incidenti di sicurezza e le violazioni dei dati personali
X	X		Gestione del personale
X	X		Istruzioni per la gestione degli strumenti
X	X		Gestione dei terzi che accedono ai dati
X	X		Trasparenza nei confronti dell'interessato

ACC: Misure valutate Accettabili
MIG: Misure valutate Migliorabili

Piano d’azione

Si ritiene che le misure tecniche ed organizzative adottate siano adeguate al rischio collegato all’attività di trattamento in esame. Occorre calendarizzare un corso di formazione ad hoc, nel quale approfondire le tematiche in materia di data protection relativamente ai sistemi di videosorveglianza in uso presso la Polizia locale.
Occorre programmare una specifica sessione formativa suppletiva per i designati e autorizzati al trattamento interni sul tema videosorveglianza e linee guida dell’EDPB.
Si ritiene di effettuare con cadenza annuale o biennale attività di audit sul responsabile del trattamento, allo scopo di verificare il rispetto dell’accordo sulla protezione dei dati personali.
Si ritiene necessario aggiornare la presente DPIA al verificarsi di una delle seguenti condizioni:

- modifica del sistema hardware e/o software in uso;
- implementazione di nuove tecnologie (ad es. di tipo intelligente o di riconoscimento biometrico tramite "Alert riconoscimento facciale", che consente la visualizzazione dei volti di una scena o la ricerca del volto in una scena in base a immagini in archivio o rilevate nel video);
- aggiornamenti normativi o chiarimenti interpretativi delle Autorità Garanti per la protezione dei dati personali;
- variazione del soggetto operante in qualità di responsabile del trattamento.

Rischi

SI	ACC	MIG	ELENCO RISCHI
X	X		Accesso illegittimo ai dati
X	X		Modifiche indesiderate dei dati
X	X		Perdita dei dati

ACC: Principi valutati Accettabili
MIG: Principi valutati Migliorabili

Piano d'azione

La considerazione del contesto in cui si sviluppa l'azione dei sistemi di videosorveglianza adottati dal Comune di NEVIANO, nonché le sue finalità, le modalità con cui avviene il trattamento dei dati e la tipologia dei medesimi e le misure giuridiche di contenimento dei rischi consentono di poter considerare il rischio per le libertà e di diritti dei cittadini di livello complessivo MEDIO (su Riservatezza) e BASSO (su Integrità e Disponibilità).
Le misure di sicurezza per la gestione del rischio sono state implementate e si ritiene che allo stato attuale, sebbene siano astrattamente idonee a far diminuire i rischi indicati nel presente documento, possano essere ulteriormente migliorate.
Il presente documento andrà integrato, altresì, ogni volta che dovesse essere rilevata qualche criticità ovvero appalesarsi la necessità di rivalutare l'adeguatezza e la conformità del funzionamento dei sistemi in uso.

PARERI

Parere DPO/RPD

L'Avv. Graziano Garrisi, nella qualità di Responsabile della Protezione Dati del Comune di NEVIANO, ha espresso il seguente parere:
In seguito ad attenta analisi del presente documento, visto l'art. 39 par. 1 lett. c) del Reg. UE 2016/679, il DPO ritiene che i rischi per i diritti e le libertà degli interessati soggetti alle riprese dei vari sistemi di videosorveglianza, 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.

Si consiglia, tuttavia, di provvedere quanto prima alla implementazione di tutte le misure di sicurezza previste dal piano d'azione indicato dall'Ente (come risultanti anche dalla relazione sullo stato di applicazione delle misure di sicurezza descritto dal fornitore che ha predisposto il sistema di videosorveglianza).

In qualità di DPO, inoltre, consiglio di monitorare e verificare periodicamente le misure di sicurezza logiche e organizzative implementate e le misure di sicurezza fisica a tutela degli apparati di videosorveglianza, nonché vigilare sul rispetto delle istruzioni date ai soggetti autorizzati al trattamento, che hanno accesso alle immagini sia in semplice visualizzazione che alle registrazioni.

Infine, si raccomanda di analizzare e revisionare (ed eventualmente aggiornare in corso "d'opera") almeno con cadenza biennale il presente documento, salvo variazioni significative dei trattamenti che comportino una necessità di aggiornamento con tempistiche inferiori all'annualità quali, ad esempio, l'individuazione di ulteriori società esterne alle quali affidare il ruolo di responsabile del trattamento ex art. 28, GDPR o l'introduzione di nuove telecamere (soprattutto se dotate di funzionalità quali l'utilizzo di sistemi di intelligenza artificiale).

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.

Parere degli interessati

Non è stato chiesto il parere degli interessati in quanto, allo stato attuale, non si ritiene necessario, essendo tali sistemi utilizzati per fini di tutela della sicurezza urbana, per la prevenzione e il contrasto dei fenomeni di criminalità diffusa e predatoria oppure per l'esecuzione di un compito di interesse pubblico posto in capo al titolare del trattamento ovvero, per il perseguimento di determinate finalità in precedenza indicate, anche nell'adempimento di quanto stabilito nel Regolamento comunale.