COMUNE DI NESPOLO

VIA ROMA 156, 02020 NESPOLO RI

DPIA

DPIA: TRATTAMENTO DEI DATI PERSONALI ATTRAVERSO ATTIVITA' DI VIDEOSORVEGLIANZA COMUNALE COMUNE DI NESPOLO

Trattamento: Sistema di videosorveglianza comunale

DPIA
Versione: 1.0
Data: 26/03/2026

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

(ex art. 35 regolamento (UE) 2016/679)

Sommario

1. INFORMAZIONI SULLA DPIA

Denominazione della DPIA: TRATTAMENTO DEI DATI PERSONALI ATTRAVERSO ATTIVITA' DI VIDEOSORVEGLIANZA COMUNALE COMUNE DI NESPOLO

Trattamento: Sistema di videosorveglianza comunale

Data di creazione: 16/03/2026

Data di validazione:16/03/2026

Redattore: Giuseppe Ciarcelluti

Revisore: Dott. Marchioni Giacomo DPO

Validatore: Comune di Nespolo Titolare Del Trattamento Nella Persona Del Sindaco Dott. Luigino Cavallari

2. PARERI

2.1. DPO

Denominazione del DPO: Dott. MARCHIONI GIACOMO

Parere: Il trattamento potrebbe essere attuato

Motivazione:

Parere Finale del Responsabile della Protezione dei Dati (DPO)

Presupposti di Liceità e Proporzionalità

In via preliminare, si attesta che il trattamento è pienamente lecito e proporzionato ai sensi del GDPR. Esso trova la sua base giuridica nell'Art. 6, par. 1, lett. e), essendo necessario per l'esecuzione di compiti di interesse pubblico quali la sicurezza urbana e la tutela del patrimonio. Il sistema rispetta rigorosamente il principio di minimizzazione (Art. 5): le riprese sono limitate agli spazi strettamente necessari, evitando intrusioni nella sfera privata, e l'impiego della tecnologia è risultato indispensabile poiché altre misure (es. presidio fisico) risulterebbero meno efficaci o eccessivamente onerose.

Valutazione Tecnica e Organizzativa

Tanto premesso, il DPO esprime parere favorevole al trattamento, fondato sulla solidità delle misure di sicurezza implementate:

Sicurezza Logica Multilivello: Sono state adottate password robuste e univoche sia per la gestione di ogni singola telecamera che per l'accesso alle immagini registrate. I profili autorizzativi sono granulari e limitati al personale specificamente formato.

Crittografia e Blindatura: L'uso della crittografia AES-256 sui flussi video e la segregazione degli apparati in locali protetti e armadi blindati garantiscono l'inviolabilità dei dati contro intercettazioni o sottrazioni fisiche.

Tracciabilità (Doppio Binario): Il controllo è garantito dall'incrocio tra i log digitali di sistema e il Registro Cartaceo degli Accessi vidimato, assicurando la piena accountability.

Trasparenza Totale: L'Ente ha assolto agli obblighi informativi tramite cartellonistica a norma EDPB, informativa estesa e una sezione dedicata sul portale istituzionale (Sezione Privacy Videosorveglianza).

Conclusioni e Raccomandazioni

Il trattamento è dichiarato pienamente legittimo e procedibile. Si raccomanda di formalizzare con Nomina ex Art. 28 GDPR ogni intervento di manutentori esterni che comporti l'accesso ai dati, fornendo loro istruzioni vincolanti, e di mantenere un programma di audit periodico sulla tenuta dei registri e sull'efficienza degli apparati.

2.2. Interessati

Non è stato richiesto il parere dei soggetti interessati o dei loro rappresentanti.

Motivo assenza parere interessati:
il trattamento messo in atto per motivi di interesse pubblico non richiede parere degli interessati.

3. CONTESTO

3.1. Panoramica

Panoramica

Denominazione del trattamento Sistema di videosorveglianza comunale

Descrizione estesa del trattamento

Il trattamento è connesso alle procedure amministrative necessarie alla gestione del Sistema di videosorveglianza comunale installato per garantire il controllo di determinate aree critiche per la sicurezza pubblica e urbana, l'identificazione, in tempo reale, di luoghi e situazioni di ingorghi per consentire il pronto intervento della Polizia municipale, assicurando la sicurezza stradale e la fluidità della circolazione, la tutela del patrimonio pubblico da atti di vandalismo e danneggiamento, il supporto alle indagini di polizia giudiziaria e l'ausilio nella ricostruzione della dinamica degli incidenti stradali. Il trattamento comprende la lettura delle targhe dei veicoli che accedono in Via Napoli e in Via Roma. Di seguito un quadro riassuntivo del posizionamento delle telecamere presenti nel territorio comunale con le specifiche tecniche.

POSTAZIONE	TIPOLOGIA CAMERA	FUNZIONALITA' SPECIFICA
1. Isola Ecologica (altezza Circ. Ovest)	Hikvision 5 MP	Monitoraggio area conferimento rifiuti
2. Via Napoli	Hikvision TCM203-A	Lettura Targhe (OCR)
3. P.zza Monumento (Girone)	Hikvision 4 MP	Monitoraggio area pubblica
4. Ingresso Cimitero Comunale	Hikvision 4 MP	Monitoraggio area sensibile
5. Via Roma	Hikvision TCM203-A	Lettura Targhe (OCR)

Finalità del trattamento

Esecuzione di un compito di pubblico interesse ; Esercizio di pubblici poteri di cui è investito il titolare del trattamento art. 6 par. e GDPR

Categorie di soggetti interessati dal trattamento

Cittadini

Titolari del trattamento

AMMINISTRAZIONE COMUNALE

Responsabili del trattamento

AMMINISTRAZIONE COMUNALE

Norme applicabili al trattamento

Decreto Legislativo 31 marzo 1998, n. 112; Regolamento (UE) n. 2016/679; Regolamento Comunale in materia di Videosorveglianza nr. 17 del 17/12/2025 ; Provvedimento del 8 aprile 2010 Garante privacy; Comitato europeo per la protezione dei dati - Linee guida 3/2019; Art. 6 e del GDPR 2016/679; Legge 18 aprile 2017, n. 48. "Disposizioni urgenti in materia di sicurezza delle città"

Valutazione del revisore Accettabile

3.2. cessi e asset di supporto

Dati, processi e asset di supporto

Descrizione dei dati trattati

Immagini; Videoregistrazioni; Targa automobilistica

Durata trattamento e conservazione dei dati personali

Durata prestabilita del trattamento: 7 Giorni. La conservazione dei dati è limitata a un massimo di 7 giorni, fatte salve le ipotesi di specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria in relazione a attività di indagine in corso.

Categorie di destinatari

Uffici giudiziari; Forze di polizia; Autorità pubblica; Soggetti terzi

Persone autorizzate al trattamento

L'OPERATORE P. L. Ag. Giseppe Ciarcelluti

Ciclo di vita dei dati

Il ciclo di vita dei dati di videosorveglianza comunale si articola in quattro fasi essenziali: l'acquisizione per finalità di pubblico interesse, la conservazione sicura limitata al tempo strettamente necessario (di norma fino a 7 giorni), l'accesso e il trattamento ristretto al personale autorizzato e per specifiche necessità, e la successiva cancellazione automatica e definitiva. La conservazione dei dati è limitata a un massimo di 7 giorni, fatte salve le ipotesi di specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria in relazione a attività di indagine in corso.

Asset di supporto dei dati

Sistema videosorveglianza; **REGISTRATORE HIK VSION MODELLO DS-7732NI-14; Videocamera, Monitor.**

Valutazione del revisore	Accettabile

4. PRINCIPI FONDAMENTALI

4.1. Proporzionalità e necessità

Finalità

Le finalità del trattamento sono esplicite, specifiche e legittime?

Finalità del Trattamento di Videosorveglianza Urbana
Il trattamento dei dati di videosorveglianza è ritenuto necessario per l'esecuzione di un compito di interesse pubblico rilevante o connesso all'esercizio di pubblici poteri, ai sensi dell'Art. 6, par. 1, lett. e) del Regolamento (UE) 2016/679 (GDPR).

Tali finalità sono molteplici e strettamente correlate al mandato istituzionale del Comune in materia di sicurezza e gestione del territorio:

Sicurezza Urbana e Pubblica: Consiste nella prevenzione e nel contrasto di attività illecite, microcriminalità, atti di vandalismo e turbative dell'ordine pubblico nelle aree accessibili al pubblico.

Tutela del Patrimonio Pubblico: Protezione di beni e strutture comunali, come parchi, edifici municipali e monumenti, per contrastare fenomeni di degrado e danneggiamento.

Controllo della Viabilità e degli Accessi Specifici:

Monitoraggio del traffico e accertamento di infrazioni al Codice della Strada (es. abbandono illecito di rifiuti).

Inoltre, il sistema di lettura targhe è specificamente funzionale al monitoraggio e alla gestione degli accessi in Via Roma e in Via Napoli del comune di Nespolo

Supporto alle Indagini e Cooperazione con le Autorità: Fornitura di dati e prove registrate alle Forze dell'Ordine e all'Autorità Giudiziaria per l'accertamento di responsabilità penali e civili, nel rispetto delle specifiche richieste.

Si conferma che le finalità di trattamento perseguite dal sistema di videosorveglianza urbana e di lettura targhe sono state valutate e risultano pienamente conformi ai requisiti stabiliti dall'Art. 5, par. 1, lett. b) del Regolamento (UE) 2016/679 (GDPR), in quanto sono:

Determinate: Sono state individuate in modo specifico in fase di progettazione e sono dettagliate nei documenti ufficiali del Comune (Regolamento e Informativa), non consentendo un utilizzo generico o futuro non previsto.

Esplicite: Vengono chiaramente definite e comunicate agli interessati (cittadini e visitatori) attraverso l'apposita cartellonistica e l'Informativa estesa, garantendo la trasparenza del trattamento.

Legittime: Sono fondate sull'esecuzione di un compito di interesse pubblico (Art. 6, par. 1, lett. e) del GDPR)
In sintesi, il Comune assicura che il trattamento dei dati personali avviene per scopi specifici, dichiarati e giuridicamente validi, escludendo l'uso dei dati per finalità diverse o incompatibili con quelle sopra stabilite.

Valutazione del revisore Accettabile

Commento di valutazione

In un'ottica di leale collaborazione istituzionale e al fine di garantire la massima coerenza del sistema di videosorveglianza con le direttive nazionali in materia di sicurezza urbana, il Comune ha provveduto a consultare preventivamente la Prefettura di Rieti con nota p.e.c. del 09/01/2026, richiedendo un parere circa l'opportunità di sottoscrivere un formale 'Patto per la Sicurezza Urbana' per l'esercizio delle due telecamere con funzionalità OCR (rilevamento targhe).

Pur in assenza di riscontro alla data di redazione della presente valutazione, l'Ente ritiene il trattamento lecito e proporzionato ai sensi dell'Art. 6, par. 1, lett. e) del GDPR, in quanto finalizzato all'esecuzione di compiti di interesse pubblico (Sicurezza Urbana e Polizia Stradale) già previsti dal vigente Regolamento Comunale

Criteri di liceità

Quali sono i principi di liceità che rendono il trattamento legittimo?

La liceità del trattamento dei dati di videosorveglianza è fondata sull'Articolo 6, paragrafo 1, lettera e) del Regolamento Generale sulla Protezione dei Dati (GDPR).

Articolo 6, par. 1, lett. e) - Esecuzione di un compito di interesse pubblico
"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 Comune, in qualità di Titolare del Trattamento, è investito dei seguenti poteri pubblici e compiti di interesse pubblico che legittimano l'uso della videosorveglianza:

Sicurezza Urbana e Ordine Pubblico: Rientra nei poteri e doveri dell'ente locale concorrere alla sicurezza urbana, come stabilito dalla normativa nazionale (es. D.L. 20/2017 convertito in L. 48/2017) e alla sicurezza pubblica Legge 18 aprile 2017, n. 48. "Disposizioni urgenti in materia di sicurezza delle città"

Tutela del Patrimonio: La protezione dei beni pubblici e del decoro urbano è un compito istituzionale specifico dell'ente comunale.

Gestione della Viabilità e Controllo Territoriale: L'installazione di sistemi di lettura targhe per il monitoraggio del traffico e la gestione degli accessi in Via Roma e in Via Napoli rientra nell'esercizio di funzioni pubbliche di regolamentazione del territorio e di gestione dei servizi.

Valutazione del revisore Accettabile

Adeguatezza e pertinenza dei dati personali

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

In conformità al principio di minimizzazione, il trattamento di videosorveglianza è configurato per raccogliere solo le immagini e i dati temporali strettamente necessari (pertinenti e adeguati) al conseguimento delle finalità di sicurezza pubblica e urbana e tutela del patrimonio; l'eventuale acquisizione di dati specifici come le targhe è limitata e giustificata esclusivamente dalla necessità di vigilanza sul traffico e di accertamento delle violazioni al Codice della Strada, prevedendo in ogni caso un tempo di conservazione ristretto per tutti i dati.

Valutazione del revisore Accettabile

Accuratezza e aggiornamento dei dati personali

I dati sono accurati e mantenuti aggiornati?

L'accuratezza e l'aggiornamento dei dati (immagini) sono garantiti dalla costante verifica della funzionalità tecnica del sistema (risoluzione e inquadratura), dalla rapida eliminazione automatica delle registrazioni inutili e dall'intervento tempestivo per la manutenzione e la calibrazione degli impianti in caso di malfunzionamento.

Valutazione del revisore Accettabile

Durata trattamento e conservazione dei dati personali

Qual è la durata della conservazione dei dati?

Il periodo di conservazione è definito in 7 giorni, ritenuto il tempo massimo indispensabile (e non eccedente) per consentire all'autorità comunale di visionare le registrazioni, espletare le verifiche necessarie e, su specifica e formale richiesta, mettere tempestivamente a disposizione le immagini alle Forze dell'Ordine, all'Autorità Giudiziaria o a terzi legittimati per l'esercizio di un diritto (ad esempio, il diritto di accesso). Trascorso tale termine e in assenza di qualsiasi richiesta di accesso o acquisizione legalmente supportata, i dati vengono eliminati automaticamente dal sistema.

Valutazione del revisore Accettabile

4.2. Misure di protezione dei diritti degli interessati

Informativa

Come sono informati i soggetti interessati riguardo al trattamento dei loro dati personali?

La trasparenza del trattamento è garantita da un sistema di informativa stratificata conforme alle Linee Guida EDPB 3/2019.

Primo livello (Informativa breve): Segnaletica di avviso installata prima del raggio di azione delle telecamere, contenente le informazioni essenziali (identità del Titolare, finalità del trattamento, presenza di sistema OCR/lettura targhe e diritti dell'interessato) mediante icone e testi sintetici. Il cartello include un QR Code per l'accesso immediato all'informativa completa tramite dispositivo mobile.

Secondo livello (Informativa estesa): Documento dettagliato pubblicato sul sito web istituzionale dell'Ente e disponibile presso il Comando di Polizia Locale, redatto ai sensi dell'art. 13 GDPR, che specifica la base giuridica, i tempi di conservazione (fissati in 7 giorni, salvo diverse esigenze di P.G.), i destinatari dei dati e i punti di contatto del DPO."

Valutazione del revisore Accettabile

Consenso

Come si ottiene il consenso dei soggetti interessati?

Il trattamento di videosorveglianza comunale non richiede il consenso degli interessati, poiché la sua liceità è fondata sull'esecuzione di un compito di interesse pubblico rilevante (Art. 6, par. 1, lett. e, GDPR).

Valutazione del revisore Accettabile

Diritto di accesso e portabilità

Come esercitano i soggetti interessati i loro diritti di accesso e alla portabilità dei dati?

L'esercizio del diritto di accesso (Art. 15 GDPR) avviene tramite richiesta formale e circostanziata indirizzata al Titolare del trattamento (il Comune), specificando data, orario e luogo della ripresa per consentire l'estrazione mirata; il diritto alla portabilità (Art. 20 GDPR) non è applicabile.

Valutazione del revisore Accettabile

Diritto di rettifica e all'oblio

Come esercitano i soggetti interessati i loro diritti alla rettifica e alla cancellazione dei dati?

Limitazioni all'esercizio dei diritti: Il Titolare dà atto che, data la natura intrinseca del trattamento (immagini e log di transito), il diritto di rettifica (art. 16 GDPR) è di fatto inapplicabile in quanto il dato raccolto (targa/transito) è una rappresentazione oggettiva di un fatto storico non modificabile. Il diritto all'oblio (art. 17 GDPR) si ritiene soddisfatto mediante la procedura di cancellazione automatica e irreversibile dei dati alla scadenza del 7° giorno di conservazione, fatte salve eventuali esigenze di conservazione ulteriore derivanti da specifiche richieste dell'Autorità Giudiziaria o di Polizia Giudiziaria.

Valutazione del revisore Accettabile

Diritto di limitazione e opposizione

Come esercitano i soggetti interessati i loro diritti di limitazione e opposizione al trattamento?

Gestione dei Diritti di Limitazione e Opposizione (Artt. 18 e 21 GDPR)
1. Diritto di Limitazione del Trattamento (Art. 18 GDPR)
L'Ente garantisce all'interessato il diritto di ottenere la limitazione del trattamento, ovvero il "contrassegno" dei dati conservati con l'obiettivo di limitarne l'elaborazione futura.

Finalità e Modalità: Qualora l'interessato contesti l'esattezza dei dati (es. errore di lettura OCR della targa) o la liceità del trattamento entro il termine di conservazione di 7 giorni, il Comune procederà all'isolamento tecnico dei log di transito e dei relativi fotogrammi.

Effetto Operativo: Tale procedura comporta la sospensione della sovrascrittura automatica (cancellazione), permettendo la conservazione del dato esclusivamente per finalità di verifica o per l'esercizio di un diritto in sede giudiziaria, sottraendolo a qualsiasi altra attività di elaborazione ordinaria.

2. Diritto di Opposizione al Trattamento (Art. 21 GDPR)
L'interessato ha il diritto di opporsi, per motivi connessi alla sua situazione particolare, al trattamento dei dati basato sull'esecuzione di un compito di interesse pubblico (Art. 6, par. 1, lett. e).

Valutazione della Prevalenza: Ai sensi dell'Art. 21, par. 1 del GDPR, il Comune, in qualità di Titolare, ha la facoltà di dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento.

Bilanciamento di Interessi: Nel contesto della videosorveglianza urbana e della lettura targhe, l'interesse pubblico alla prevenzione dei reati, alla tutela del patrimonio e alla sicurezza stradale — finalità per le quali è stata avviata anche l'interlocuzione conoscitiva con la Prefettura — è ritenuto, di norma, prevalente rispetto ai diritti individuali, salvo casi eccezionali e motivati che saranno oggetto di puntuale esame istruttorio.

3. Strumenti e Requisiti per l'Esercizio dei Diritti
Per garantire l'effettività di tali diritti, l'Ente ha stabilito le seguenti procedure:

Modulistica Dedicata: L'istanza deve essere presentata utilizzando esclusivamente la modulistica specifica per l'esercizio dei diritti dell'interessato, predisposta e messa a disposizione dal Comune sul portale istituzionale o presso il Comando di Polizia Locale.

Identificazione e Legittimazione: L'interessato deve allegare copia di un documento di identità e fornire prova documentale della titolarità o della legittima disponibilità del veicolo (es. carta di circolazione, contratto di noleggio) riferita alla data e all'orario del transito. Tali elementi sono indispensabili per evitare l'accesso indebito a dati di terzi.

Canali di Ricezione: La richiesta deve essere inviata tramite PEC istituzionale o depositata presso l'Ufficio Protocollo. Il Comune fornirà riscontro motivato entro il termine di 30 giorni dal ricevimento

Valutazione del revisore Accettabile

Contrattualizzazione del responsabile del trattamento

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e formalizzati in un contratto?

Si dà atto che, alla data di redazione della presente valutazione, il Comune non ha proceduto alla nomina di soggetti esterni quali Responsabili del Trattamento ai sensi dell'Art. 28 del GDPR, in quanto le attività di gestione e controllo del sistema sono attualmente rimesse esclusivamente al personale interno autorizzato.

Valutazione del revisore Da migliorare

Commento di valutazione

Il DPO esprime parere favorevole in merito alla procedura di verifica programmata dall'Ente, ritenendola conforme al principio di Accountability (art. 24 GDPR). Si evidenzia che la mancata nomina del manutentore è legittima esclusivamente nel caso in cui siano adottate misure tecniche e organizzative tali da inibire oggettivamente l'accesso ai dati personali (es. separazione fisica dei database durante gli interventi o supervisione costante del personale autorizzato).

Tuttavia, il DPO raccomanda che l'esito di tale verifica venga formalizzato in un breve verbale tecnico sottoscritto dal Comandante della Polizia Locale/Responsabile Tecnico, al fine di documentare le ragioni della mancata contrattualizzazione ex art. 28 GDPR e di comprovare l'assenza di rischi per la riservatezza degli interessati durante le operazioni di manutenzione

Piano di azione / Azioni correttive

L'Ente verificherà con estremo rigore le modalità operative con cui verrà espletata la manutenzione tecnica dell'impianto: qualora tali interventi comportino, anche solo potenzialmente o accidentalmente, l'accesso ai dati personali (immagini o log dei transiti), si procederà tempestivamente alla formale contrattualizzazione del manutentore quale Responsabile Esterno del Trattamento. Viceversa, qualora sia tecnicamente garantito che l'attività di manutenzione riguardi esclusivamente la componente hardware (ottiche, sostegni, cablaggi) e avvenga senza alcuna possibilità di accesso o visualizzazione dei dati memorizzati nel software di gestione, non si renderà necessario il perfezionamento della predetta nomina.

Trasferimento dei dati personali

I dati sono adeguatamente protetti nel caso di trasferimento al di fuori dell'Unione Europea?

I dati personali non sono trasferiti fuori dell' Unione Europea.

Valutazione del revisore Accettabile

5. RISCHI E MISURE DI SICUREZZA

5.1. Misure esistenti o pianificate

Monitoraggio dello stato delle apparecchiature

Descrizione

E' garantito il monitoraggio continuo dello stato di funzionamento e dell'integrità delle apparecchiature (telecamere, server e supporti di memorizzazione) al fine di garantire la qualità costante e l'accuratezza dei dati video raccolti, come nuova misura di sicurezza.

Valutazione del revisore Accettabile

Contenitori con serrature a chiave

Descrizione

Al fine di massimizzare la protezione dei dati e prevenire accessi non autorizzati, il dispositivo di registrazione (NVR/Server) è collocato all'interno di un locale tecnico dedicato, non accessibile al pubblico e protetto da chiusura fissa. All'interno di tale ambiente, l'apparato è ulteriormente segregato in un armadio rack blindato dotato di serratura a chiave.

L'accesso sia al locale tecnico che al contenitore rack è esclusivamente riservato al Comandante della Polizia Locale pro tempore, in qualità di soggetto designato, e al personale espressamente autorizzato. Tale configurazione 'a doppio livello' garantisce la massima resilienza contro tentativi di manomissione, sottrazione dei supporti di memoria o estrazione illecita di dati tramite periferiche esterne.

Valutazione del revisore Accettabile

Commento di valutazione

Il DPO valuta l'adozione di un locale dedicato e di un armadio rack chiuso a chiave come una misura di sicurezza fisica eccellente e pienamente conforme al principio di 'Security by Design'. La presenza di un doppio perimetro di protezione riduce drasticamente il rischio di Data Breach derivante da intrusione fisica.

Sotto il profilo del controllo, il DPO raccomanda che l'accesso a tale stanza venga limitato esclusivamente alle finalità strettamente connesse alla gestione del sistema o a indifferibili esigenze tecniche, mantenendo traccia (anche informale) degli ingressi dei soggetti non abituali (es. tecnici manutentori).

Autenticazione utenti

Descrizione

L'accesso alle funzionalità del software di gestione e alle immagini archiviate è regolato da un sistema di autenticazione forte. Ogni soggetto autorizzato accede tramite credenziali univoche e personali (User ID e Password), impedendo l'utilizzo di account condivisi e garantendo la tracciabilità delle operazioni effettuate.

Il sistema impone una politica di password complesse in linea con i più recenti standard di sicurezza informatica, prevedendo:

Lunghezza minima di 12 caratteri;

Combinazione obbligatoria di caratteri alfanumerici (maiuscole, minuscole, numeri) e caratteri speciali.

L'Ente prevede inoltre la rotazione periodica delle credenziali e la disattivazione immediata degli account in caso di cessazione del rapporto di servizio o cambio di mansione del personale autorizzato.
Tracciabilità delle Operazioni e Log di Sistema
1. Log di Accesso Informatico (Logging Elettronico)

Il sistema software di gestione è configurato per la registrazione automatica dei log di accesso. Tali file registrano l'ID utente, la data, l'orario e le operazioni compiute (es. visualizzazione live, consultazione archivio, esportazione). In conformità ai principi di accountability e alle indicazioni del Garante Privacy, questi log sono conservati per un periodo di 6 mesi, termine ritenuto congruo per consentire verifiche postume sulla liceità dei trattamenti ed eventuali accertamenti di Polizia Giudiziaria o disciplinari. Al termine del periodo, i log vengono sovrascritti o cancellati automaticamente.

2. Tracciabilità Fisica (Registro Cartaceo degli Accessi)

A integrazione e rafforzamento dei log informatici, considerata la struttura organizzativa dell'Ente e al fine di garantire una tracciabilità immediata e incontestabile, l'Ente istituisce un Registro Cartaceo degli Accessi.

Il Registro, con pagine numerate e vidimate dal Comandante della Polizia Locale, è custodito nel locale tecnico dove risiede l'apparato di registrazione. Ogni operatore autorizzato è obbligato ad annotare manualmente per ogni singola sessione:

Data e ora dell'accesso e dell'uscita;

Identità del soggetto che accede;

Motivazione specifica dell'operazione (es. manutenzione ordinaria, estrazione immagini su delega di P.G., verifica tecnica).

La coesistenza dei log elettronici (6 mesi) e del registro cartaceo assicura un doppio livello di verifica, garantendo la massima trasparenza nella gestione dell'impianto.

Valutazione del revisore Accettabile

Commento di valutazione

Il DPO valuta positivamente la strategia di tracciabilità 'a doppio binario' adottata dall'Ente. La conservazione dei log elettronici per 6 mesi soddisfa i requisiti di sicurezza logica previsti dal GDPR, mentre l'istituzione del registro cartaceo rappresenta una misura organizzativa d'eccellenza per la realtà di un micro-comune.

Tale combinazione riduce drasticamente il rischio di accessi abusivi 'silenziosi', poiché ogni operazione digitale deve trovare corrispondenza in una firma fisica. Si raccomanda che il registro cartaceo, una volta completato, venga archiviato in modo sicuro per un periodo coerente con i termini di prescrizione amministrativa (almeno 5 anni), a fini di documentazione del corretto operato dell'Ente.

Formazione del personale

Descrizione

Per garantire la corretta e lecita gestione del trattamento, è previsto un corso di formazione specifico e periodico per il personale autorizzato (Incaricati) che accede al sistema di videosorveglianza, focalizzato sulle procedure operative, sugli obblighi di sicurezza e sul rispetto della normativa vigente in materia di privacy (GDPR).

Valutazione del revisore Accettabile

Sistema antincendio

Descrizione

A protezione del locale che ospita le apparecchiature sensibili e il registratore, è presente e attivo un sistema antincendio conforme alle normative vigenti, quale misura essenziale di sicurezza fisica contro il rischio di distruzione o danneggiamento dei dati.

Valutazione del revisore Accettabile

Assegnazione degli incarichi

Descrizione

L'incarico per la supervisione e la gestione operativa del trattamento dei dati di videosorveglianza è stato formalmente assegnato (Incaricato del Trattamento) al Comandante della Polizia Locale, che ne assume la piena responsabilità esecutiva.

Valutazione del revisore Accettabile

Verifiche periodiche delle procedure

Descrizione

Sono previste verifiche periodiche delle procedure operative e delle misure di sicurezza del sistema di videosorveglianza con cadenza almeno semestrale, al fine di assicurare la continua conformità al GDPR e l'efficacia del trattamento.

Valutazione del revisore Accettabile

Certificazione degli impianti

Descrizione

Gli impianti di videosorveglianza sono certificati da tecnici abilitati, confermando la loro installazione a regola d'arte e la piena conformità alle normative tecniche e di sicurezza vigenti (incluse le norme CEI e le disposizioni del DM 37/08).

Valutazione del revisore Accettabile

Registrazione degli accessi fisici

Descrizione

Gli accessi fisici al locale che ospita il registratore e le apparecchiature sono rigorosamente monitorati e tracciati attraverso un registro degli accessi, garantendo piena accountability su chi e quando ha avuto accesso al sistema.

Valutazione del revisore Accettabile

Protezione dei locali con serrature di sicurezza

Descrizione

L'accesso ai locali sensibili di conservazione e gestione del sistema è protetto da serrature di sicurezza ed è strettamente limitato al personale autorizzato, con le chiavi in dotazione e sotto la custodia esclusiva dell'Operatore P.L., Ag. Ciarcelluti Giuseppe.

Valutazione del revisore Accettabile

Crittografia dei dati

Descrizione

Al fine di prevenire l'intercettazione dei dati durante la trasmissione tra le telecamere e la centrale di registrazione, l'Ente adotta sistemi di Trasporto Dati Cifrato. Nello specifico, i flussi video inviati tramite ponti radio (operanti su banda 5GHz con apparati Mikrotik SXT 5) sono protetti dai seguenti protocolli di sicurezza avanzata:

Cifratura di tipo WPA3: Standard di sicurezza wireless di ultima generazione che garantisce una protezione superiore contro i tentativi di accesso non autorizzati alla rete radio.

Algoritmo di Criptazione AES-256 bit: Il traffico dati è cifrato secondo lo standard Advanced Encryption Standard con chiave a 256 bit, garantendo la riservatezza e l'integrità dei flussi video in ottemperanza ai provvedimenti del Garante per la Privacy in materia di sicurezza delle trasmissioni.

Valutazione del revisore Accettabile

Commento di valutazione

Il DPO valuta positivamente le soluzioni tecniche scelte per proteggere i dati. L'uso dei sistemi di cifratura più recenti (WPA3 e AES-256) garantisce che le immagini e le targhe dei veicoli non possano essere intercettate o visualizzate da estranei mentre passano via radio dalle telecamere al Comune.

Questa misura assicura che le informazioni viaggino sempre in modo protetto e 'illeggibile' per chiunque non sia autorizzato, garantendo la massima riservatezza fin dalla trasmissione. Il DPO raccomanda al Comune di chiedere periodicamente ai tecnici di aggiornare i software degli apparati radio, così da mantenere il sistema sempre protetto contro i nuovi rischi informatici

Monitoraggio dello stato delle apparecchiature

Descrizione

Ogni telecamera installata sul territorio è protetta da una password di accesso individuale e univoca. Questo significa che le credenziali di accesso cambiano per ogni singolo apparato. Tale misura impedisce che la violazione o la manomissione di una singola telecamera possa compromettere l'intero sistema di sorveglianza o consentire l'accesso non autorizzato alle altre componenti della rete comunale

Valutazione del revisore Accettabile

Commento di valutazione

Il DPO accoglie con favore questa ulteriore protezione. L'uso di password diverse per ogni telecamera è una scelta molto prudente: evita il cosiddetto 'effetto domino', dove la scoperta di una sola chiave di accesso metterebbe a rischio tutto l'impianto.

Si tratta di una misura di sicurezza concreta che dimostra l'attenzione del Comune nel proteggere ogni punto del sistema, anche quelli fisicamente distanti dalla sede municipale. Il DPO raccomanda di conservare l'elenco di queste password in modo sicuro e criptato, limitandone la conoscenza al solo personale tecnico incaricato

5.2. Rischi

Accesso illegittimo ai dati

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

Il principale impatto sugli interessati sarebbe la violazione della riservatezza e la potenziale discriminazione o danno alla reputazione, derivanti dalla diffusione non autorizzata delle immagini che rivelano la loro presenza, spostamenti o comportamenti in un luogo pubblico.

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

Uso non autorizzato o negligente della strumentazione; Trattamento (volontario o inconsapevole) non consentito di dati (personali); Furto di documenti o supporti di memorizzazione; Errore nello svolgimento di mansioni (per ignoranza delle procedure di gestione, carenza di consapevolezza, disattenzione o incuria); Accesso non autorizzato alla rete (anche tramite AP wireless non autorizzati)

Quali sono le fonti di rischio?

Le principali minacce per la riservatezza dei dati sono state individuate in tre aree critiche:

L'accesso fisico e informatico esterno, legato a possibili tentativi di manomissione delle telecamere in strada, intercettazione dei segnali radio o intrusioni nel locale tecnico;

Il rischio operativo, connesso agli interventi di manutenzione da parte di ditte esterne che potrebbero accedere al software per scopi tecnici;

Il fattore umano, ovvero il rischio che il personale autorizzato consulti le immagini per scopi diversi da quelli istituzionali

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

Assegnazione degli incarichi; Autenticazione utenti; Formazione del personale; Protezione dei locali con serrature di sicurezza; Crittografia dei dati; Monitoraggio dello stato delle apparecchiature

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

Indicare i motivi del valore stimato di gravità del rischio

Nonostante queste potenziali minacce, l'adozione di password diverse per ogni telecamera, l'uso di segnali radio criptati, il doppio perimetro di chiusura a chiave dei server e l'obbligo di firma sul registro cartaceo riducono drasticamente la probabilità che questi rischi si trasformino in una reale violazione dei dati (Data Breach). Il sistema è quindi progettato per rendere ogni accesso illegittimo estremamente difficile da attuare e, in ogni caso, immediatamente tracciabile.

Come si stimerebbe la probabilità del rischio, con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? Limitata

Indicare i motivi del valore stimato di probabilità del rischio

La combinazione di controlli tecnici strutturali (isolamento della rete e crittografia pianificata) con i controlli procedurali e organizzativi (formazione e tracciabilità) fa sì che la probabilità di un accesso illegittimo con esito positivo sia stimata come Limitata.

Valutazione del revisore Accettabile

Modifica non desiderata dei dati

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

La modifica non desiderata dei dati rappresenta un rischio critico, poiché potrebbe compromettere la validità legale delle riprese. Gli impatti principali sono individuati in:

Perdita di efficacia probatoria: L'alterazione di un fotogramma o di un log renderebbe le immagini inutilizzabili come prova in sede giudiziaria o amministrativa.

Impossibilità di ricostruire gli eventi: La cancellazione selettiva di alcuni transiti impedirebbe alla Polizia Locale di svolgere correttamente le indagini.

Lesione dei diritti degli interessati: Una modifica accidentale potrebbe portare all'errata identificazione di un veicolo o di un soggetto, causando un danno ingiusto al cittadino.

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

Uso non autorizzato o negligente della strumentazione; Accesso non autorizzato alla rete; Uso non autorizzato della rete da parte degli utenti o abuso delle autorizzazioni; Trattamento (volontario o inconsapevole) non consentito di dati (personali); Degrado dei supporti di memorizzazione (per esempio memorie di massa, archivi cartacei); Furto di apparati o componenti; Errore nello svolgimento di mansioni (per ignoranza delle procedure di gestione, carenza di consapevolezza, disattenzione o incuria); Distruzione di strumentazione da parte di malintenzionati o per errore o disattenzione; Incendio

Quali sono le fonti di rischio?

Il rischio di manomissione e alterazione delle registrazioni video deriva da una combinazione di fattori, che spaziano dalle minacce umane (personale infedele o attacchi informatici esterni) fino a guasti tecnici hardware/software e eventi ambientali catastrofici.

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

Sistema antincendio; Assegnazione degli incarichi; Verifiche periodiche delle procedure; Certificazione degli impianti; Monitoraggio dello stato delle apparecchiature; Contenitori con serrature a chiave; Autenticazione utenti; Formazione del personale; Registrazione degli accessi fisici; Protezione dei locali con serrature di sicurezza; Crittografia dei dati

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

Indicare i motivi del valore stimato di gravità del rischio

La gravità di una possibile modifica indesiderata dei dati è stimata come limitata in quanto il sistema di videosorveglianza adotta un formato di registrazione 'proprietario' e non editabile, che impedisce tecnicamente a chiunque di alterare i singoli fotogrammi o le sequenze video. Inoltre, poiché le funzioni di cancellazione e configurazione sono protette da password di livello amministratore (detenute esclusivamente dal Comandante) e ogni accesso fisico è tracciato sul registro cartaceo vidimato, la possibilità che avvenga una manipolazione dei dati senza lasciare traccia o che tale modifica comprometta l'intero sistema è da considerarsi estremamente remota

Come si stimerebbe la probabilità del rischio, con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? Limitata

Indicare i motivi del valore stimato di probabilità del rischio

La minaccia di modifica indesiderata dei dati è stimata come limitata poiché il sistema è protetto da barriere tecniche che rendono la manomissione dei file quasi impossibile nella pratica quotidiana.

Nello specifico, i filmati sono salvati in un formato digitale 'blindato' (non modificabile con normali programmi di video-editing) e le funzioni di cancellazione o modifica sono disabilitate per tutti gli operatori, essendo accessibili solo tramite una password di alto livello custodita dal Comandante. Inoltre, la presenza del registro cartaceo numerato impedisce di eliminare o alterare le registrazioni in modo furtivo, poiché ogni operazione lascerebbe un'incongruenza immediata tra il registro fisico e il contenuto del disco fisso.

Perdita dei dati

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

La perdita d dei dati di videosorveglianza mina l'integrità della prova, esponendo l'interessato al rischio di ingiustizia, danno reputazionale e perdita di tutele legali e finanziarie, compromettendo il diritto fondamentale alla verità e al controllo sui propri dati personali.

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

Uso non autorizzato o negligente della strumentazione; Accesso non autorizzato alla rete (anche tramite AP wireless non autorizzati); Trattamento (volontario o inconsapevole) non consentito di dati (personali); Uso dei servizi da parte di persone non autorizzate o elevamento di privilegi (privilege escalation); Degrado dei supporti di memorizzazione (per esempio memorie di massa, archivi cartacei); Uso di servizi in modo non autorizzato; Furto di apparati o componenti; Incendio; Allagamento; Perdita di energia elettrica (o sbalzi di tensione)

Quali sono le fonti di rischio?

Analisi delle Fonti di Rischio: Perdita di Disponibilità e Integrità
"Le principali fonti di rischio per la disponibilità dei dati sono riconducibili a guasti hardware ed eventi esogeni (usura dei supporti, sovratensioni elettriche o sinistri nei locali tecnici), nonché a potenziali errori umani commessi dal personale autorizzato o dai tecnici in fase di manutenzione (cancellazioni accidentali, errate configurazioni o distacchi impropri dei cablaggi).

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

Sistema antincendio; Assegnazione degli incarichi; Verifiche periodiche delle procedure; Certificazione degli impianti; Monitoraggio dello stato delle apparecchiature; Contenitori con serrature a chiave; Autenticazione utenti; Formazione del personale; Registrazione degli accessi fisici; Protezione dei locali con serrature di sicurezza; Crittografia dei dati

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

Indicare i motivi del valore stimato di gravità del rischio

La probabilità che si verifichi una perdita di dati o un accesso illegittimo è stimata come estremamente bassa, in quanto suffragata da un sistema di protezione a più livelli che agisce su ogni punto di vulnerabilità identificato.

Nello specifico:

La resilienza elettrica e la scelta di hardware professionale neutralizzano i rischi di guasto tecnico e perdita accidentale;

La blindatura fisica (locale tecnico e armadi rack chiusi a chiave) impedisce la sottrazione dei supporti;

La protezione logica (crittografia AES-256 e password univoche per ogni telecamera) rende vani i tentativi di intercettazione esterna.

La robustezza di tali misure, unita al controllo umano garantito dall'obbligo di firma sul registro degli accessi, permette di affermare che il rischio residuo è ridotto ai minimi termini tecnologici e organizzativi oggi possibili.

Come si stimerebbe la probabilità del rischio, con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? Limitata

Indicare i motivi del valore stimato di probabilità del rischio

le minacce fisiche sono neutralizzate dal confinamento dei dispositivi di archiviazione in stanze chiuse a chiave, e il rischio di guasto o vulnerabilità è minimizzato dalla manutenzione regolare degli apparati e dalla formazione costante del personale dai presidi contro le cause di danneggiamento fisico e da una manutenzione programmata

Valutazione del revisore Accettabile

6. PIANO DI AZIONE

Contrattualizzazione del responsabile del trattamento

Piano di azione / Azioni correttive

L'Ente verificherà con estremo rigore le modalità operative con cui verrà espletata la manutenzione tecnica dell'impianto: qualora tali interventi comportino, anche solo potenzialmente o accidentalmente, l'accesso ai dati personali (immagini o log dei transiti), si procederà tempestivamente alla formale contrattualizzazione del manutentore quale Responsabile Esterno del Trattamento. Viceversa, qualora sia tecnicamente garantito che l'attività di manutenzione riguardi esclusivamente la componente hardware (ottiche, sostegni, cablaggi) e avvenga senza alcuna possibilità di accesso o visualizzazione dei dati memorizzati nel software di gestione, non si renderà necessario il perfezionamento della predetta nomina.

Data prevista per l'attuazione	30.04.2026
	L'Operatore P.L. Ag.
Responsabile dell'attuazione	
	Giuseppe Ciarcelluti

7. VALIDAZIONE

Io sottoscritto Sindaco del comune di Nespolo Titolare del trattamento dati in qualità di rappresentante legale e in qualità di soggetto validatore della DPIA relativa al trattamento Sistema di videosorveglianza comunale, dopo aver esaminato l'intera valutazione d'impatto effettuata:

- Confermo che la descrizione del contesto del trattamento è coerente con la realtà
- Confermo di aver preso nota dei rischi esistenti in base alle misure pianificate o esistenti
- Ritengo non rilevante o non fondato il parere negativo espresso dagli interessati
- Approvo le misure correttive indicate
- Mi impegno ad attuare quanto prima le misure correttive indicate

Firma del Validatore della DPIA e data

Il Sindaco Dott. Luigino Cavallari

Firmato digitalmente da:
Cavallari Luigino
Firmato il 25/03/2026 13:46
Seriale Certificato: 3789237
Valido dal 20/08/2024 al 20/08/2027
InfoCamere Qualified Electronic Signature CA

IL redattore

L'Operatore P.L. Istr. Giuseppe Ciarcelluti **Firma**

Il DPO. F.to. digitalmente

Dott. Giacomo Marchioni

Nespolo ...../...../.....