



Monte San Giovanni in Sabina

Viale Regina Margherita, 2- 02040 Monte San Giovanni in Sabina (RI)

DPIA

**DPIA: TRATTAMENTO DEI DATI PERSONALI ATTIVITA' DI VIDEOSORVEGLIANZA COMUNALE
COMUNE DI MONTE SAN GIOVANNI IN SABINA**

Trattamento: Sistema di videosorveglianza comunale

Data: 10/09/2026

Versione: 1.0



VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

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

Sommario

1.	INFORMAZIONI SULLA DPIA	3
2.	PARERI	3
2.1.	DPO	3
2.2.	Interessati	4
3.	CONTESTO	4
3.1.	Panoramica	4
3.2.	Dati, processi e asset di supporto	6
4.	PRINCIPI FONDAMENTALI	6
4.1.	Proporzionalità e necessità	6
4.2.	Misure di protezione dei diritti degli interessati	10
5.	RISCHI E MISURE DI SICUREZZA	13
5.1.	Misure esistenti o pianificate	13
5.2.	Rischi	17
6.	VALIDAZIONE	20

1. INFORMAZIONI SULLA DPIA

Denominazione della DPIA: TRATTAMENTO DEI DATI PERSONALI ATTIVITA' DI VIDEOSORVEGLIANZA COMUNALE
COMUNE DI MONTE SAN GIOVANNI IN SABINA

Trattamento: Sistema di videosorveglianza comunale

Data di creazione: 10/09/2026

Data di validazione: 11/09/2026

Redattore: Responsabile Ufficio Tecnico Comunale EMILIANO BIANCHI

Revisore: DPO.

Validatore: Comune di Monte San Giovanni in Sabina Titolare del trattamento dei dati personali

2. PARERI

2.1. DPO

Denominazione del DPO: MARCHIONI GIACOMO

Parere: Il trattamento può essere attuato

Motivazione:

Il sottoscritto DPO, esaminata la DPIA relativa al sistema di videosorveglianza comunale, esprime **parere favorevole** al trattamento, confermandone la conformità agli Artt. 5, 6, 12, 13, 14, 24, 25, 28, 30, 32 e 35 del GDPR.

L'attivazione del sistema risponde a legittime finalità di sicurezza urbana, tutela del patrimonio pubblico e prevenzione di illeciti ambientali. Tale operatività è pienamente conforme al **Regolamento Comunale sulla Videosorveglianza vigente** formalmente approvato dall'Ente con Deliberazione di Consiglio Comunale n. 21 del 08/06/2018 per disciplinare le modalità di trattamento e l'esercizio dei diritti. Il trattamento si attesta come proporzionato e lecito, basato su quanto segue:

- **Basi Giuridiche e Trasparenza (Artt. 12, 13 e 14):** Il trattamento trova fondamento nell'Art. 6, comma 1, lett. e) del GDPR (esecuzione di un compito di interesse pubblico). Il principio di trasparenza è attuato mediante un modello di informativa a due livelli, pienamente conforme alle linee guida del Garante:
 1. **Informativa "breve" (primo livello):** Garantita da cartellonistica ad alta visibilità posizionata in prossimità delle aree videosorvegliate, contenente gli elementi essenziali e un QR-code/link diretto per l'approfondimento.
 2. **Informativa "estesa" (secondo livello):** Pubblicata in modo permanente e facilmente accessibile nella sezione "Privacy" del sito web istituzionale, contenente tutti i dettagli richiesti dagli Artt. 13 e 14 (identità del Titolare, contatti del DPO, finalità del trattamento, base giuridica, tempi di conservazione e modalità di esercizio dei diritti).
- **Gestione Interna e Profili Autorizzativi (Artt. 24, 29 e 32):** L'accesso ai flussi video è riservato esclusivamente al personale interno espressamente autorizzato e formalmente istruito mediante apposite nomine e istruzioni operative scritte. Ogni accesso è rigorosamente tracciato tramite:
 - **Registro cartaceo degli accessi:** Annotazione sistematica di data, ora, operatore e finalità della consultazione.
 - **Verbale di estrazione:** Documento obbligatorio per ogni esportazione di immagini, che attesta la necessità dell'operazione e la finalità istituzionale dell'intervento.
- **Misure di Sicurezza e Log (Art. 32):** Il sistema adotta misure tecniche all'avanguardia: trasmissione dei flussi in modalità cifrata tramite tunnel VPN IPSec su APN privato, crittografia dei volumi di archiviazione (*Data atRest*), credenziali di accesso univoche per ogni dispositivo e protezione fisica degli apparati di registrazione. La segmentazione logica impedisce che la manomissione di

una singola telecamera possa compromettere l'intera rete. Il sistema garantisce inoltre la tracciabilità delle operazioni attraverso log inalterabili e protetti, che registrano ogni accesso e attività effettuata, consentendo una revisione periodica e un controllo puntuale su chi abbia visualizzato o estratto le immagini.

- **Gestione dei Fornitori (Art. 28):** Il Titolare ha formalizzato l'impegno alla nomina della ditta installatrice e di manutenzione quale Responsabile del Trattamento ex Art. 28 GDPR, vincolandola contrattualmente al divieto di accesso ingiustificato, all'obbligo di riservatezza, alla notifica dei *data breach* e al divieto di trasferimento dati extra-SEE.
- **Conservazione e Diritti (Artt. 5, 15-22):** Il principio di limitazione della conservazione è garantito dalla cancellazione automatica dei dati dopo 7 giorni. Le procedure interne assicurano l'esercizio dei diritti degli interessati in piena conformità agli Artt. 15 e seguenti del GDPR.

Il trattamento è pertanto ritenuto lecito, sicuro e conforme alle prescrizioni del Regolamento UE 2016/679.

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	

Panoramica

Il trattamento posto in essere dal Comune di Monte San Giovanni in Sabina consiste nel monitoraggio sistematico di aree strategiche del territorio mediante dispositivi di ripresa digitale a ottica fissa. L'attività esclude categoricamente il monitoraggio in tempo reale ed è limitata alla sola visione ed estrazione dei filmati registrati. Le immagini consentono la rilevazione visiva ex-post dei transiti veicolari e delle relative targhe, con totale esclusione di software OCR per la lettura automatica o di sistemi di analisi biometrica.

Tale attività è finalizzata alla tutela della sicurezza urbana e dell'ordine pubblico, alla prevenzione e repressione di atti di vandalismo e danneggiamento del patrimonio pubblico, nonché al contrasto dei fenomeni di abbandono incontrollato di rifiuti, a garanzia del decoro urbano e della salute pubblica; il sistema persegue altresì finalità di sicurezza stradale, consentendo il monitoraggio dei flussi di traffico e l'accertamento delle violazioni inerenti alla circolazione veicolare nel territorio dell'Ente, secondo le finalità espresse nell'informativa istituzionale.

Il sistema si compone complessivamente di 3 dispositivi di ripresa situati presso:

LOCALITA' MOLETTA

LOCALITA' GALLO

LOCALITA' SANTO PIETRO

Il sistema di videosorveglianza prevede una rete di trasmissione basata su tecnologia 4G/LTE, in cui il flusso dei dati è protetto mediante tunnel VPN IPSec e protocollo TLS 1.2+. Tale architettura garantisce la cifratura end-to-end dei dati, rendendo il traffico illeggibile e inaccessibile da parte di terzi durante il transito dalla periferia al centro di controllo. L'infrastruttura è segregata tramite APN privato, garantendo l'isolamento logico del sistema rispetto alla rete internet pubblica. In relazione a ciò si allega la relazione tecnica fornita dalla ditta installatrice.

Finalità del trattamento

Esecuzione di un compito di pubblico interesse ; Esercizio di pubblici poteri di cui è investito il titolare del trattamento Articolo 6, paragrafo 1, lettera e) del GDPR

Categorie di soggetti interessati dal trattamento

Cittadini; Personale dipendente

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 08/06/2018; Provvedimento del 8 aprile 2010; Comitato europeo per la protezione dei dati - Linee guida 3/2019; Art. 6 e del GDPR 2016/679; Legge 18 aprile 2017, n. 48.

Valutazione del revisore

Accettabile

3.2. Dati, processi 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

Categorie di destinatari

Uffici giudiziari; Forze di polizia; Autorità pubblica; Soggetti terzi, Fornitori nominati Responsabili del trattamento art. 28 GDPR

Persone autorizzate al trattamento

Sindaco pro tempore del Comune di Monte San Giovanni in Sabina Sig.ra Marcella Santoni e il dipendente comunale Sig.ra Graziella Giovanna Ruggeri.

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; Videocamere, sistema di registrazione

Valutazione del revisore

Accettabile

4. PRINCIPI FONDAMENTALI

4.1. Proporzionalità e necessità

Finalità

Le finalità del trattamento sono esplicite, specifiche e legittime?

Il trattamento persegue finalità di interesse pubblico (Art. 6.1, lett. e del GDPR), con particolare riferimento a:

Sicurezza Pubblica e Urbana, Supporto Investigativo: Prevenzione e repressione dei reati, tutela dell'ordine pubblico e supporto fondamentale alle attività di indagine della Polizia Giudiziaria e delle Forze dell'Ordine dello Stato.

Sicurezza Urbana e Decoro: Prevenzione di atti vandalici, danneggiamento del patrimonio pubblico e tutela dei beni della comunità.

Tutela Ambientale: Contrasto all'abbandono incontrollato di rifiuti in aree critiche del territorio comunale (isole ecologiche/cassette rifiuti).

Sicurezza Stradale: Monitoraggio dei flussi veicolari ed eventuale supporto all'accertamento di violazioni inerenti la circolazione nel territorio dell'Ente.

Proporzionalità e Necessità

Il sistema è stato progettato nel pieno rispetto del principio di minimizzazione dei dati:

Necessità: Il controllo del territorio tramite presenza fisica non è attuabile. Il Comune non dispone di personale di polizia locale; la videosorveglianza basata sulla registrazione delle immagini costituisce l'unico strumento idoneo a garantire un presidio costante, un efficace deterrente e la documentazione oggettiva degli illeciti.

Proporzionalità Spaziale: Il posizionamento dei dispositivi è stato definito in modo da presidiare esclusivamente gli accessi e i punti di transito nevralgici del territorio comunale, garantendo così il controllo dei varchi d'ingresso più importanti. Il campo visivo di ogni telecamera è limitato allo stretto necessario per la finalità di sicurezza urbana.

Proporzionalità Temporale: La conservazione dei dati è limitata a un massimo di 7 giorni (168 ore). Tale termine è strettamente congruo e necessario per consentire la ricezione delle segnalazioni, l'analisi ex-post e l'estrazione dei filmati, tenendo conto dell'articolazione del territorio e dei turni di servizio del personale (Soggetti Autorizzati) preposto alla gestione in continuità operativa. Decorso tale termine, avviene la sovrascrittura automatica.

Tipologia Dati: Il sistema registra esclusivamente le immagini dei transiti e consente la sola lettura visiva delle targhe ex-post. Non è attivo alcun automatismo sanzionatorio collegato a banche dati esterne (come il controllo automatico in tempo reale di assicurazioni/revisioni), né alcun tracciamento sistematico degli spostamenti. I dati vengono verificati e analizzati solo a posteriori, in caso di illecito o specifica necessità di indagine.

Valutazione del revisore

Accettabile

Commento di valutazione

Le finalità dichiarate rientrano pienamente nei compiti istituzionali del Comune e la videosorveglianza basata sulla registrazione delle immagini risulta lo strumento più idoneo a garantire il presidio e la documentazione oggettiva degli eventi nelle aree critiche del territorio.

I requisiti di necessità e proporzionalità sono pienamente rispettati: l'assenza di automatismi sanzionatori diretti o di incroci massivi con banche dati esterne esclude il rischio di sorveglianza ingiustificata o tracciamento sistematico dei cittadini.

L'accesso ai dati registrati, limitato ai Soggetti Autorizzati secondo le finalità espresse nell'informativa e per sole esigenze ex-post, bilancia correttamente le esigenze di sicurezza pubblica e urbana con la tutela dei diritti degli interessati. Il trattamento è pertanto valutato come proporzionato, necessario e pienamente conforme alla normativa vigente.

Criteri di liceità

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

Principi di Liceità, Correttezza e Trasparenza

Il trattamento dei dati personali effettuato tramite il sistema di videosorveglianza comunale si conforma rigorosamente ai principi stabiliti dall'Art. 5 del Regolamento UE 2016/679:

Liceità: Il trattamento trova la sua base giuridica nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (Art. 6, par. 1, lett. e del GDPR) e nell'adempimento delle funzioni istituzionali dell'Ente in materia di Polizia Locale, sicurezza urbana (D.L. 14/2017), sicurezza pubblica, codice della strada e gestione dei rifiuti/tutela ambientale (D.Lgs. 152/2006).

Correttezza: L'Amministrazione utilizza le immagini esclusivamente per le finalità dichiarate e secondo le competenze individuate, escludendo qualsiasi uso secondario incompatibile, eccedente o non conforme rispetto agli scopi istituzionali prefissati.

Trasparenza: Il principio è garantito mediante un sistema di informativa a più livelli:

Informativa di primo livello: In ottemperanza all'Art. 13 del GDPR, la cartellonistica informativa è posizionata preventivamente rispetto al raggio d'azione dei dispositivi. Ogni cartello riporta chiaramente la finalità del trattamento, l'identità del Titolare del trattamento e le modalità per accedere all'informativa estesa. Quest'ultima è resa disponibile tramite un codice QR dedicato che rimanda direttamente alla sezione 'Videosorveglianza' del sito istituzionale del Comune, dove sono dettagliati i tempi di conservazione dei dati (fissati in 7 giorni), i riferimenti di contatto del Data Protection Officer (DPO) e i contatti istituzionali dell'Ente.

Informativa di secondo livello: Tale documentazione, redatta in conformità all'Art. 13 del GDPR, è costantemente disponibile e consultabile sul sito istituzionale dell'Ente e presso gli uffici comunali. Essa integra le informazioni sintetiche presenti sulla cartellonistica, fornendo il dettaglio completo relativo alle finalità del trattamento, alla base giuridica, ai tempi di conservazione, ai soggetti autorizzati al trattamento, nonché le modalità specifiche tramite cui l'interessato può esercitare i propri diritti (accesso, rettifica, limitazione, opposizione alla cancellazione).

Limitazione della conservazione: Il sistema è configurato per la cancellazione automatica e definitiva dei dati decorse le 168 ore (7 giorni), termine congruo e giustificato dalle esigenze organizzative dell'Ente, fatte salve le specifiche richieste dell'Autorità Giudiziaria o di Polizia Giudiziaria.

Integrità e Riservatezza: La sicurezza dei dati è garantita da misure tecniche adeguate, tra cui l'interconnessione di tutti i dispositivi tramite canali cifrati in modalità VPN dedicata per azzerare i rischi di accesso abusivo, e da misure organizzative stringenti, quali la limitazione dell'accesso alla visione e all'estrazione ai Soggetti Autorizzati, con tracciamento di ogni attività sia tramite log di sistema sia tramite registro interno.

Valutazione del revisore

Accettabile

Commento di valutazione

I principi generali di protezione dei dati sono pienamente rispettati. L'impianto normativo citato giustifica correttamente l'azione del Comune, mentre la trasparenza verso la cittadinanza è assicurata in modo efficace dal doppio livello di informativa (breve sul territorio ed estesa sul sito web).

La sicurezza dei flussi video è garantita dall'isolamento logico su APN dedicato e dalla cifratura VPN IPSec end-to-end, che rende i dati inaccessibili a terzi. L'integrità e la tracciabilità delle consultazioni ex-post sono assicurate da un sistema di autenticazione con audit-log immutabile. L'intera infrastruttura garantisce pertanto piena conformità ai principi di cui all'Art. 5 del GDPR.

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)?

Adeguatezza e pertinenza dei dati

Il sistema garantisce che il trattamento sia costantemente limitato ai soli dati strettamente necessari rispetto alle finalità perseguite:

Qualità e Tipologia dei dati: Si acquisiscono esclusivamente immagini video e fotogrammi relativi ai transiti. È categoricamente esclusa la raccolta di dati audio, dati biometrici o categorie particolari di dati personali (Art. 9 GDPR).

Inquadratura e Angolazione: I dispositivi a ottica fissa sono orientati in modo selettivo esclusivamente sulle porzioni di aree pubbliche interessate (varchi d'ingresso), riducendo al minimo la ripresa di dettagli o soggetti non pertinenti.

Risoluzione e Zoom: La risoluzione delle immagini è configurata per il solo accertamento ex-post degli illeciti (es. lettura visiva della targa o individuazione del sacco dei rifiuti abbandonato). Essendo i dispositivi a ottica fissa, non è possibile effettuare zoom ottici o brandeggi; l'eventuale ingrandimento digitale è limitato alla fase di estrazione dei fotogrammi d'interesse.

Esclusione di funzionalità superflue o invasive: Non sono attivi software di intelligenza artificiale per l'analisi predittiva o del comportamento delle persone, né sistemi di tracciamento sistematico, lettura automatica OCR o riconoscimento facciale.

Valutazione del revisore

Accettabile

Commento di valutazione

Le misure di minimizzazione applicate sono pienamente adeguate. L'esclusione categorica di funzionalità invasive, quali intelligenza artificiale, OCR o tracciamento facciale, riduce al minimo l'impatto sui cittadini, assicurando la piena conformità al principio di pertinenza dei dati.

Accuratezza e aggiornamento dei dati personali

I dati sono accurati e mantenuti aggiornati?

Sincronizzazione (NTP): Le 3 postazioni e l'NVR/SERVER si sincronizzano con server orari ufficiali, garantendo la precisione temporale necessaria alla validità probatoria.

Manutenzione: Il Responsabile del trattamento, vincolato da clausole contrattuali ex Art. 28 GDPR, assicura l'accuratezza e la nitidezza delle riprese tramite manutenzioni periodiche.

Ciclo di vita: Le immagini sono riproduzioni fedeli di eventi puntuali, prive di necessità di aggiornamento e soggette a cancellazione automatica dopo 7 giorni.

Valutazione del revisore

Accettabile

Commento di valutazione

L'esattezza dei dati è pienamente garantita. La sincronizzazione automatica dell'orario assicura il valore legale delle registrazioni, mentre la manutenzione regolare delle telecamere mantiene le immagini nitide ed evita errori di identificazione. Il trattamento rispetta i requisiti del GDPR.

Durata trattamento e conservazione dei dati personali

Qual è la durata della conservazione dei dati?

Termine di conservazione: Il periodo di conservazione dei dati è fissato in un massimo di 7 giorni (168 ore), termine ritenuto strettamente necessario e proporzionato rispetto alle finalità dell'Ente. Questo lasso di tempo è tecnicamente e organizzativamente giustificato dall'articolazione dei turni di servizio del personale preposto (Soggetti Autorizzati) in regime di continuità operativa.

Finalità del termine: Tale durata consente alle forze dell'ordine di rilevare gli illeciti (es. abbandono di rifiuti), di istruire le relative procedure sanzionatorie e di rispondere con congruo margine di tempo alle richieste di acquisizione documentale da parte dell'Autorità Giudiziaria o di altre Forze dell'ordine.

Cancellazione automatica: Allo scadere del 7° giorno, le immagini vengono eliminate automaticamente dal sistema tramite sovrascrittura irreversibile.

Deroghe e limitazioni d'accesso: La conservazione si protrae oltre i 7 giorni esclusivamente per i fotogrammi o i filmati specifici oggetto di indagine, a seguito di formali richieste degli organi inquirenti o per l'avvio di procedimenti sanzionatori diretti da parte delle forze dell'ordine. È categoricamente escluso l'accesso diretto, la visione o il prelievo delle immagini da parte di soggetti privati o comunque estranei alle funzioni di polizia e vigilanza.

Valutazione del revisore

Accettabile

Commento di valutazione

Il termine di 7 giorni rispetta pienamente i principi di proporzionalità e limitazione della conservazione. È correttamente bilanciato tra le esigenze organizzative dell'Ente e la necessità di accertamento degli illeciti. I sistemi di cancellazione automatica e il divieto di accesso ai privati escludono rischi di conservazione ingiustificata, rendendo il processo pienamente conforme al GDPR.

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 a due livelli (stratificata):

Informativa di primo livello: In ottemperanza all'Art. 13 del GDPR, la cartellonistica informativa è posizionata preventivamente rispetto al raggio d'azione dei dispositivi. Ogni cartello riporta chiaramente la finalità del trattamento, l'identità del Titolare del trattamento e le modalità per accedere all'informativa estesa. Quest'ultima è resa disponibile tramite un codice QR dedicato che rimanda direttamente alla sezione 'Videosorveglianza' del sito istituzionale del Comune, dove sono dettagliati i tempi di conservazione dei dati (fissati in 7 giorni), i riferimenti di contatto del Data Protection Officer (DPO) e i contatti istituzionali dell'Ente.

Informativa di secondo livello: Tale documentazione, redatta in conformità all'Art. 13 del GDPR, è costantemente disponibile e consultabile sul sito istituzionale dell'Ente e presso gli uffici comunali. Essa integra le informazioni sintetiche presenti sulla cartellonistica, fornendo il dettaglio completo relativo alle finalità del trattamento, alla base giuridica, ai tempi di conservazione, ai soggetti autorizzati al trattamento, nonché le modalità specifiche tramite cui l'interessato può esercitare i propri diritti (accesso, rettifica, limitazione, opposizione alla cancellazione).

Valutazione del revisore

Accettabile

Commento di valutazione

La modalità informativa scelta è conforme. Il rinvio presente sul cartello fisico alla sezione web dedicata per i dettagli di contatto del DPO risponde a criteri di efficacia e flessibilità organizzativa, garantendo al cittadino il reperimento di informazioni sempre aggiornate ed evitando l'obsolescenza della cartellonistica stradale.

Consenso

Come si ottiene il consenso dei soggetti interessati?

Inapplicabilità del consenso: Il trattamento dei dati personali effettuato tramite il sistema di videosorveglianza comunale non richiede, né potrebbe basarsi sul consenso degli interessati, data la natura pubblica dei luoghi monitorati.

Base giuridica prevalente: La liceità del trattamento si fonda esclusivamente sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (Art. 6, par. 1, lett. e del GDPR), in combinato disposto con le funzioni istituzionali dell'Ente in materia di Polizia Locale, sicurezza urbana e tutela ambientale.

Bilanciamento dei diritti: La tutela dei diritti dei cittadini è pienamente garantita dall'adempimento rigoroso degli obblighi di trasparenza (informativa preventiva sul territorio). In merito al diritto di opposizione (Art. 21 GDPR), lo stesso deve ritenersi generalmente limitato o inapplicabile, prevalendo l'interesse pubblico superiore alla prevenzione e all'accertamento degli illeciti amministrativi e penali.

Valutazione del revisore

Accettabile

Commento di valutazione

La base giuridica individuata è corretta e conforme. Il trattamento non necessita del consenso degli interessati poiché risponde a finalità di interesse pubblico e a compiti istituzionali dell'Ente. Il bilanciamento tra l'azione amministrativa e i diritti dei cittadini è assicurato dalla trasparenza delle informative, escludendo rischi di trattamenti arbitrari.

Diritto di accesso e portabilità

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

Diritto di Accesso (Art. 15 GDPR): L'esercizio del diritto di accesso avviene tramite richiesta formale e dettagliata al Comune. L'interessato deve specificare con esattezza la data, l'orario e il luogo del transito per consentire l'estrazione mirata del filmato. L'accesso è condizionato alla reale disponibilità dei dati (entro il limite dei 7 giorni di conservazione) e al rispetto della riservatezza dei terzi: qualora nel filmato siano presenti altri soggetti, volti o targhe, il Comune procederà all'oscuramento/pixelatura dei dati non pertinenti prima dell'ostensione.

Diritto alla Portabilità (Art. 20 GDPR): Tale diritto è categoricamente non applicabile al presente trattamento. Ai sensi dell'Art. 20, par. 3 del GDPR, la portabilità è esclusa per tutti i trattamenti necessari all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare.

Valutazione del revisore

Accettabile

Commento di valutazione

Le procedure previste per la gestione dei diritti sono pienamente conformi. Il diritto di accesso è correttamente disciplinato per evitare la divulgazione di dati di terzi (tramite oscuramento) e l'esclusione del diritto alla portabilità rispetta fedelmente i limiti normativi previsti dall'Art. 20 del GDPR per i trattamenti di interesse pubblico.

Diritto di rettifica e all'oblio

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

Rettifica (Art. 16 GDPR): Non applicabile. Le immagini registrate rappresentano un fatto storico oggettivo. Non è tecnicamente né giuridicamente possibile modificare o alterare una registrazione video senza comprometterne l'integrità e la validità come prova.

Cancellazione / Oblio (Art. 17 GDPR):

Profilo tecnico: Il diritto è assorbito dal sistema stesso, che provvede alla cancellazione automatica e irreversibile di tutti i dati allo scadere rigoroso dei 7 giorni.

Profilo giuridico: Non è ammessa la cancellazione anticipata su richiesta del singolo. Prevale l'interesse pubblico alla prevenzione e accertamento degli illeciti (es. abbandono rifiuti); consentire l'eliminazione immediata dei fotogrammi su istanza di parte vanificherebbe l'efficacia stessa delle funzioni di controllo e di tutela dell'ordine pubblico.

Valutazione del revisore

Accettabile

Commento di valutazione

L'analisi dei diritti di rettifica e cancellazione risponde perfettamente ai canoni interpretativi del Garante in materia di videosorveglianza pubblica. È corretto rilevare l'inapplicabilità materiale della rettifica su dati video/storici. Sotto il profilo della cancellazione, il bilanciamento è ottimale: la sovrascrittura automatica a 7 giorni garantisce l'oblio standard, mentre la limitazione alla cancellazione anticipata protegge l'efficacia delle funzioni di controllo del Comune da richieste pretestuose.

Diritto di limitazione e opposizione

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

Limitazione (Art. 18 GDPR): Applicabile in via d'eccezione. Qualora l'interessato ne faccia richiesta per accertare, esercitare o difendere un diritto in sede giudiziaria, il Comune provvede a estrarre e isolare temporaneamente lo specifico frammento video, bloccandone la cancellazione automatica. Il resto dell'impianto prosegue con la regolare sovrascrittura a 7 giorni.

Opposizione (Art. 21 GDPR): Generalmente non applicabile. Il cittadino può opporsi al trattamento per motivi particolari, ma l'istanza viene respinta poiché l'interesse pubblico dell'Ente (sicurezza urbana e pubblica contrasto all'abbandono di rifiuti) prevale sui diritti del singolo, rendendo il controllo del territorio necessario e non interrompibile.

Modalità di esercizio: Le istanze vanno inoltrate via PEC o Protocollo, indicando data, ora e luogo esatto del transito. Per tutelare la privacy di terzi e consentire la ricerca mirata, l'interessato deve fornire elementi certi per il proprio riconoscimento (es. numero di targa o dettagli identificativi). Il riscontro avviene entro il termine massimo di 30 giorni.

Valutazione del revisore

Accettabile

Commento di valutazione

Le procedure per la gestione della limitazione e dell'opposizione sono conformi. È correttamente previsto l'isolamento del solo dato d'interesse in caso di limitazione, evitando l'alterazione dei flussi generali. Il diritto di opposizione trova il legittimo limite nella prevalenza delle funzioni dei competenti organi ispettivi e di controllo dell'Ente, mentre i requisiti di identificazione garantiscono la tutela dei dati di terzi estranei.

Contrattualizzazione del responsabile del trattamento

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

Gestione interna: La gestione operativa ordinaria e la visualizzazione delle immagini sono riservate esclusivamente al personale interno del Comune, formalmente autorizzato e istruito.

Fornitori esterni: L'Ente ha individuato nella ditta installatrice e di manutenzione il partner tecnologico di riferimento. Il Comune procederà alla formale nomina della suddetta ditta quale Responsabile del Trattamento (ex Art. 28 GDPR), vincolandola contrattualmente a standard di sicurezza rigorosi.

Garanzie: L'atto di nomina, che sarà sottoscritto prima dell'avvio del trattamento, imporrà al fornitore il divieto di accesso non autorizzato ai dati, l'obbligo di riservatezza per tutto il personale tecnico, la notifica tempestiva di eventuali data breach e l'impegno a garantire che l'intera infrastruttura operi in modalità locale, escludendo il trasferimento di dati verso server esterni o al di fuori dello Spazio Economico Europeo (SEE)

Valutazione del revisore	Accettabile
Commento di valutazione	
La sezione evidenzia una corretta gestione del rischio "a monte". La scelta di subordinare l'attivazione dei servizi tecnologici esterni alla firma preventiva degli atti ex Art. 28 GDPR garantisce la piena conformità giuridica dell'Ente. Le misure contrattuali previste assicurano che i fornitori operino come meri esecutori documentati, sotto il controllo diretto del Titolare.	

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
Misura prevista: È garantito il monitoraggio periodico dello stato di funzionamento e dell'integrità delle apparecchiature (telecamere, server e memoria) per assicurare la continuità del servizio e l'accuratezza dei dati video raccolti.
Modalità operative: La verifica viene eseguita tramite controlli visivi manuali e periodici (con cadenza sistematica) sulla funzionalità delle inquadrature, sullo stato dei dischi e sulla corretta registrazione dei flussi. La gestione di eventuali anomalie rilevate e la richiesta di intervento tecnico immediato sono in capo al Responsabile dell'Ufficio Tecnico.

Valutazione del revisore	Accettabile
Commento di valutazione	

La misura basata su controlli visivi periodici e manuali è commisurata alla dimensione dell'Ente e alla complessità dell'impianto. La designazione di un responsabile interno per l'attivazione immediata dell'assistenza tecnica garantisce una gestione adeguata dei tempi di ripristino in caso di guasto.

Contenitori con serrature a chiave

Descrizione

Segregazione fisica (Doppio livello): Al fine di prevenire accessi fisici non autorizzati, manomissioni o furti dei supporti di memoria, il dispositivo di registrazione locale (NVR/Server) è collocato all'interno di un locale dell'Ente non accessibile al pubblico e protetto da porta con serratura. All'interno di tale ambiente, l'apparato è ulteriormente segregato in un armadio rack metallico dotato di chiave di sicurezza.

Abilitazioni all'accesso e gestione chiavi: L'accesso al locale e l'apertura dell'armadio rack sono tassativamente riservati al Responsabile dell'Ufficio Tecnico e al personale autorizzato. Eventuali tecnici esterni incaricati della manutenzione possono accedere alle apparecchiature esclusivamente previa autorizzazione e sotto la diretta vigilanza del personale interno abilitato.

Valutazione del revisore

Accettabile

Commento di valutazione

La misura di sicurezza fisica adottata rispetta pienamente i requisiti dell'Art. 32 GDPR in materia di resilienza e protezione contro accessi abusivi. La combinazione del locale tecnico protetto e del rack blindato a chiave neutralizza i rischi di manomissione locale sull'hardware di rete che alimenta il Cloud. La precisazione sulle modalità di accesso per il manutentore garantisce la coerenza logica con il piano d'azione.

Autenticazione utenti

Descrizione

Credenziali univoche: L'accesso al software è consentito solo tramite credenziali personali (User ID e Password complesse di almeno 12 caratteri alfanumerici e speciali) assegnate ai soggetti autorizzati, vietando account condivisi e disattivandoli al cambio di mansione.

Log elettronici: Il sistema registra automaticamente gli accessi e le operazioni sui video (live, archivio, esportazione), conservando i log per 6 mesi prima della cancellazione automatica.

Registro cartaceo: A integrazione dei log, gli accessi fisici vengono registrati manualmente su un registro cartaceo con pagine numerate e vidimate dal Responsabile dell'Ufficio Tecnico, custodito nel locale tecnico. La compilazione del registro è di competenza di entrambi i soggetti a seconda di chi effettua l'accesso.

Verbale di estrazione: Ogni esportazione di immagini deve essere formalizzata tramite un apposito verbale che traccia l'operazione e garantisce la catena di custodia; la redazione del verbale è di competenza di entrambi i soggetti operanti.

Valutazione del revisore

Accettabile

Commento di valutazione

Il sistema combinato di credenziali personali per i soggetti autorizzati, affiancato da log a 6 mesi, registro cartaceo vidimato e verbali di estrazione — entrambi gestiti e compilati da entrambe le figure a seconda delle rispettive operazioni — garantisce la piena tracciabilità e la legittimità di ogni accesso ai dati video.

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 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

Nomina e Atto di designazione: L'Ente ha formalizzato le responsabilità dei soggetti che accedono ai dati tramite atti scritti di nomina.

Istruzioni operative: Negli atti di nomina sono espressamente indicate le istruzioni vincolanti sui limiti del trattamento, sui tempi di conservazione delle immagini, sul divieto di diffusione non autorizzata e sulle modalità di utilizzo delle credenziali personali e di compilazione dei registri/verbali.

Valutazione del revisore

Accettabile

Commento di valutazione

L'attribuzione formale dei ruoli e delle relative istruzioni operative per iscritto agli autorizzati, garantisce la piena conformità al principio di liceità e responsabilizzazione (Accountability), assicurando che il personale operi esclusivamente nei limiti e secondo le modalità definite dall'Ente.

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). Vedere relazione tecnica allegata.

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

Protezione degli accessi fisici: Il locale dell'Ente in cui sono ospitate le apparecchiature di registrazione (Server/NVR) è dotato di una porta ad anima solida dotata di serratura di sicurezza. Il locale rimane costantemente chiuso a chiave e l'accesso è interdetto al pubblico e al personale non espressamente abilitato.

Gestione e custodia delle chiavi: Le chiavi fisiche di accesso al locale sono custodite e gestite esclusivamente dai soggetti autorizzati, al fine di impedire ingressi non tracciabili o la duplicazione non autorizzata delle stesse.

Valutazione del revisore

Accettabile

Crittografia dei dati

Descrizione

Crittografia dei dati salvati (Data at Rest): Le immagini memorizzate sull'NVR/SERVER sono protette da cifratura. In caso di furto o accesso fisico non autorizzato ai dischi, i file risulteranno illeggibili e inaccessibili.

Crittografia durante l'invio (Data in Transit): I video viaggiano dalle postazioni all'NVR/SERVER attraverso un tunnel VPN dedicato. Questa protezione rende impossibile intercettare o visualizzare i flussi video mentre transitano sulla rete.

Valutazione del revisore

Accettabile

Commento di valutazione

L'uso combinato della crittografia dei dischi e di canali di trasmissione protetti tramite VPN garantisce l'assoluta riservatezza dei dati, neutralizzando i rischi di intercettazione dei flussi video in rete e di lettura dei dati in caso di furto fisico degli apparati

Monitoraggio dello stato delle apparecchiature

Descrizione

Credenziali univoche per singola telecamera: Ogni telecamera installata sul territorio è protetta da una password di accesso individuale e univoca, differenziando le credenziali per ogni singolo apparato.

Prevenzione della compromissione di rete: 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

L'adozione di password univoche e differenziate per ciascuna telecamera sul territorio isola efficacemente i singoli punti di ripresa, azzerando il rischio che la manomissione fisica o informatica di un unico apparato periferico possa compromettere la sicurezza dell'intera rete comunale.

5.2. Rischi

Accesso illegittimo ai dati

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

Violazione della riservatezza: La compromissione dei dati comporterebbe un'immediata perdita di controllo sulla sfera privata dei cittadini, rivelando dettagliati pattern di presenza e spostamenti all'interno degli spazi pubblici.

Danni alla reputazione e potenziali discriminazioni: La diffusione non autorizzata o la manipolazione delle immagini video potrebbe esporre gli interessati a giudizi distorti, lesioni della dignità personale, fino a concreti rischi di discriminazione o danni reputazionali in ambito sociale o lavorativo.

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?

Personale interno: Utilizzo improprio o fuori dalle finalità da parte delle figure autorizzate. Rischio mitigato da nomine, istruzioni vincolanti e log elettronici.

Attacchi informatici esterni: Intercettazione dei flussi video verso il Cloud o accessi abusivi alla rete. Rischio neutralizzato da connessioni VPN, protocolli cifrati e password univoche per ogni telecamera.

Intrusioni fisiche e manomissioni: Accesso abusivo al locale tecnico o manomissione delle telecamere. Rischio mitigato da serrature di sicurezza, registro cartaceo e crittografia dei dischi (Data at Rest).

Guasti tecnici o eventi accidentali: Guasti agli hard disk, interruzioni di corrente o errori orari. Rischio mitigato dal monitoraggio periodico delle apparecchiature.

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, rete dedicata

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

Trascurabile

Indicare i motivi del valore stimato di gravità del rischio

Assenza di dati sensibili o particolari: Il sistema tratta esclusivamente immagini video standard in aree pubbliche, senza l'uso di tecnologie biometriche o di riconoscimento facciale, limitando l'impatto alla sola immagine visiva.

Impossibilità di utilizzo illecito dei dati: Grazie alla crittografia a riposo (Data at Rest) e in transito (tramite VPN), anche in caso di furto fisico dei dischi o di intercettazione di rete, i filmati rimangono cifrati e totalmente illeggibili da parte di terzi non autorizzati.

Controllo totale e tracciabilità: L'accesso alle immagini è strettamente limitato a due sole figure formalmente istruite (Responsabile Tecnico e Vigile). Ogni singola operazione è tracciata in modo ridondante sia dai log elettronici inalterabili per 6 mesi, sia dal registro cartaceo vidimato, azzerando il rischio di abusi o diffusioni incontrollate.

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

Trascurabile

Indicare i motivi del valore stimato di probabilità del rischio

Massima riduzione del rischio di rete: L'uso di connessioni VPN dedicate e cifrate, unito a password individuali e univoche per ogni singola telecamera, riduce al livello minimo possibile la probabilità di un attacco informatico o di un'intercettazione esterna.

Controllo d'accesso rigoroso ed ermetico: Gli accessi fisici sono protetti da barriere strutturali (locali con serrature di sicurezza), mentre gli accessi digitali sono limitati a sole due utenze individuali (Responsabile Tecnico e Vigile) costantemente monitorate da log elettronici e registri cartacei.

Prevenzione attiva e monitoraggio: Il controllo periodico dello stato delle apparecchiature permette di intercettare e risolvere immediatamente qualsiasi anomalia o vulnerabilità tecnica prima che possa essere sfruttata.

Valutazione del revisore

Accettabile

Commento di valutazione

Nonostante l'accesso abusivo alle immagini della videosorveglianza comunale presenti una gravità teorica rilevante per la riservatezza dei cittadini, il rischio effettivo è ridotto a livelli trascurabili. L'azione combinata di misure fisiche (locali protetti), informatiche (connessioni VPN, crittografia dei dischi e password univoche per ogni telecamera) e organizzative (tracciamento tramite log e registro cartaceo per le sole due figure autorizzate) garantisce l'assoluta protezione dei dati da tentativi di intrusione esterni o interni.

Modifica non desiderata dei dati

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

Perdita di efficacia delle tutele e delle prove: L'alterazione, la cancellazione o la manipolazione dei filmati impedirebbe l'utilizzo delle immagini come prova valida in sede giudiziaria o per le attività di polizia giudiziaria del Vigile, privando i cittadini della tutela della loro sicurezza e dei loro diritti in caso di illeciti sul territorio.

Lesione dell'affidamento istituzionale: Un'eventuale manomissione dei dati o dei log di sistema minerebbe la fiducia dei cittadini nei confronti del Comune, generando un danno reputazionale legato alla percezione di una scarsa affidabilità nella gestione delle infrastrutture pubbliche e della sicurezza urbana.

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); 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?

Trascurabile

Indicare i motivi del valore stimato di gravità del rischio

Assorbimento totale del danno tramite misure tecniche: L'adozione della cifratura dei dati e di sistemi di archiviazione protetti da sovrascritture arbitrarie neutralizza alla radice l'impatto potenziale di una perdita o modifica del dato, garantendo la costante disponibilità e l'integrità dei filmati nei tempi di legge.

Inalterabilità della prova e tutela del diritto di difesa: Il rischio di compromettere la validità legale delle immagini (essenziale per la difesa dei cittadini o per l'azione del Vigile) è annullato. I log elettronici di controllo sono cifrati e inalterabili per 6 mesi, impedendo qualsiasi manipolazione silente o non tracciata.

Doppio controllo incrociato con valore legale: La presenza del registro cartaceo vidimato, aggiornato in tempo reale e co-firmato dal Responsabile Tecnico e dal Vigile a ogni accesso, assicura l'autenticità assoluta della catena di custodia dei dati. Qualsiasi anomalia verrebbe intercettata all'istante, rendendo l'impatto effettivo sui diritti degli interessati nullo o puramente teorico.

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

Trascurabile

Indicare i motivi del valore stimato di probabilità del rischio

Con riguardo alle fonti di rischio e alle minacce: Le potenziali fonti di rischio (errori/abusi del personale interno, attacchi informatici esterni o guasti tecnici) che potrebbero tentare di modificare o cancellare i dati sono state isolate e neutralizzate all'origine. La minaccia di un'alterazione silente o di un attacco esterno è resa un'ipotesi puramente teorica.

Con riguardo alle misure pianificate: La probabilità che l'evento si verifichi è stimata come "Trascurabile" grazie alla presenza di barriere di sicurezza informatiche, fisiche e organizzative estremamente stringenti:

Isolamento della rete (VPN): L'uso di canali cifrati e dedicati, unito a password individuali e univoche per ogni singola telecamera, riduce al minimo la superficie di attacco informatico esterno.

Controllo degli accessi ed ermeticità: Gli accessi digitali sono limitati rigorosamente a sole due utenze individuali, mentre i dispositivi fisici (NVR/SERVER) sono blindati all'interno di locali protetti da serrature di sicurezza.

Prevenzione e Tracciabilità totale: La presenza di log elettronici di controllo cifrati e inalterabili per 6 mesi, unita all'obbligo di compilazione del registro cartaceo d'accesso vidimato, permette un controllo periodico e incrociato costante, intercettando sul nascere qualsiasi anomalia prima che possa tradursi in un rischio concreto.

Valutazione del revisore

Accettabile

Perdita dei dati

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

Compromissione della prova e tutela legale: La perdita dei dati di videosorveglianza mina l'integrità della prova, esponendo l'interessato al rischio di ingiustizia e alla perdita di tutele legali e finanziarie.

Danno reputazionale e diritto alla verità: L'indisponibilità delle immagini può causare un danno reputazionale ingiustificato al cittadino, compromettendo il suo diritto fondamentale alla verità sui fatti accaduti.

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?

Fattori tecnici: Guasti hardware degli hard disk (NVR/SERVER), black-out elettrici prolungati con corruzione dei file, o crash del software di registrazione.

Eventi esterni accidentali: Furto fisico dei registratori, incendi, allagamenti, atti vandalici o calamità naturali che distruggono i dispositivi di memoria.

Errori umani o attacchi: Errori del personale (cancellazioni accidentali) o attacchi informatici (ransomware/malware) che criptano o eliminano i video.

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, rete dedicata.

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

Trascurabile

Indicare i motivi del valore stimato di gravità del rischio

L'impatto reale viene ridotto al minimo e reso trascurabile dalle contromisure. I dispositivi NVR/SERVER e gli hard disk sono protetti da continuità elettrica (UPS) contro i guasti, e installati dentro armadi rack blindati e stanze chiuse a chiave per impedire furti fisici o vandalismi. La manutenzione periodica hardware garantisce la costante integrità e disponibilità dei dati, contenendo gli effetti di un potenziale incidente entro livelli non significativi.

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

Trascurabile

Indicare i motivi del valore stimato di probabilità del rischio

Minacce e Fonti di rischio: Le minacce di perdita dei dati (guasti tecnici, furti hardware, errori umani o black-out) sono state isolate e rese un'ipotesi puramente teorica.

Misure pianificate: La probabilità che l'evento si verifichi è ridotta al minimo grazie a contromisure specifiche:

Protezione fisica ed elettrica: Gli NVR/SERVER sono chiusi in armadi blindati in locali protetti e supportati da gruppi di continuità (UPS) che prevengono i guasti da sbalzi di tensione.

Manutenzione e Restrizioni: La manutenzione tecnica è periodica e l'accesso fisico ai sistemi è consentito solo agli autorizzati, azzerando la probabilità di errori umani o manomissioni interne.

Valutazione del revisore

Accettabile

Commento di valutazione

Il rischio di perdita dei dati è stimato come Trascurabile sia per Gravità che per Probabilità. L'adozione di protezioni fisiche (armadi blindati e locali chiusi), elettriche (gruppi UPS) e le rigide restrizioni d'accesso riducono al minimo la possibilità di guasti o furti, garantendo la costante disponibilità dei filmati e la totale tutela dei diritti dei cittadini.

6. VALIDAZIONE

COMUNE DI MONTE SAN GIOVANNI IN SABINA

Provincia di Rieti

VERBALE DI APPROVAZIONE E VALIDAZIONE DELLA VALUTAZIONE DI IMPATTO (DPIA)

OGGETTO: Valutazione di Impatto sulla Protezione dei Dati (DPIA) relativa al sistema di videosorveglianza comunale – Parere del DPO e Validazione del Titolare.

Il giorno 11/09/2026, presso la sede municipale di Monte San Giovanni in Sabina, in riferimento alla Valutazione di Impatto sulla Protezione dei Dati (DPIA) relativa al sistema di videosorveglianza territoriale in uso al Comune;

PARERE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO) Il DPO, a seguito dell'esame tecnico-normativo condotto sull'infrastruttura e sulla documentazione prodotta inserito nelle premesse:

- Conferma che la descrizione del contesto del trattamento è coerente con la realtà operativa.
- Conferma di aver preso nota dei rischi esistenti in base alle misure pianificate o esistenti, ritenendole adeguate.
- Ritiene non rilevante o non fondato l'eventuale parere negativo espresso dagli interessati, alla luce delle preminenti finalità di tutela del territorio. Sulla base di ciò, il DPO esprime **parere favorevole** all'avvio del trattamento.

VALIDAZIONE DEL TITOLARE DEL TRATTAMENTO (IL COMUNE) Preso atto del parere favorevole rilasciato dal DPO e verificata la coerenza dell'impianto con le finalità istituzionali dell'Ente, **il Comune di Monte San Giovanni in Sabina**, in qualità di Titolare del Trattamento, **approva e valida formalmente** la presente DPIA, autorizzando l'operatività del sistema di videosorveglianza nel rispetto delle misure di sicurezza prescritte.

Il DPO (Data Protection Officer)

FIRMATO DIGITALMENTE

.....

IL RESPONSABILE DEL SERVIZIO

Firmato digitalmente da:
Bianchi Emiliano
Firmato il 11/09/2026 10:55
Seriale Certificato: 5581966
Valido dal 30/01/2026 al 30/01/2029
InfoCamere Qualified Electronic Signature CA

Sig.ra MARCELLA SANTONI

IL TITOLARE DEL TRATTAMENTO IL SINDACO PRO TEMPORE *(Per approvazione e validazione formale)*

Firmato digitalmente da:
Santoni Marcella
Firmato il 11/09/2026 10:54
Seriale Certificato: 5402483
Valido dal 14/01/2026 al 14/01/2029
InfoCamere Qualified Electronic Signature CA

