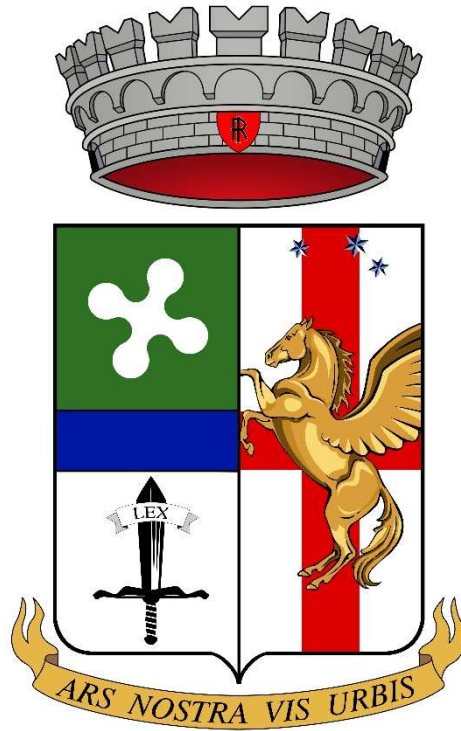




**Valutazione di impatto
sul trattamento dei dati personali
relativi al sistema di videosorveglianza
in dotazione al Corpo Intercomunale
di Polizia Locale dei comuni di
Pieve Emanuele e Sizzano**

Sommario

1 Introduzione

1.1 Oggetto e scopo

1.2 Versione

1.3 La valutazione di impatto sulla protezione dei dati (DPIA)

1.4 Le Linee Guida in materia di DPIA (LG-DPIA)

1.5 Le Linee Guida sulla videosorveglianza (LG-VS)

1.6 Obbligatorietà della DPIA per la videosorveglianza della Polizia Locale

1.7 Struttura della DPIA e sua conformità al GDPR

1.8 Abbreviazioni

2 Descrizione del trattamento

2.1 Contesto e finalità

2.1.1 Il Regolamento comunale per l'utilizzo di impianti di videosorveglianza (RCVS)

2.2 Ciclo di vita dei dati personali trattati

2.2.1 Raccolta

2.2.2 Trasmissione

2.2.3 Elaborazione e visualizzazione

2.2.4 Distribuzione

2.2.5 Conservazione e cancellazione

2.3 Misure organizzative

2.3.1 Titolare del trattamento

2.3.2 Responsabile della Protezione dei Dati

2.3.3 Soggetti autorizzati

2.3.4 Responsabili esterni

2.3.5 Amministratori di Sistema

2.3.6 Registro dei trattamenti

2.4 Tipologie di VSS in utilizzo

2.5 Videosorveglianza del territorio

2.5.1 Telecamere

2.5.2 Sistema centrale

2.5.3 Accesso alle immagini

2.6 Lettura targhe

2.6.1 Telecamere

2.6.2 Sistema centrale

2.6.3 Accesso alle immagini

2.7 Telecamere mobili per lettura targhe

2.7.1 Telecamere

2.7.2 Accesso alle immagini

2.8 Telecamere controllo infrazioni passaggio con semaforo rosso

2.8.1 Telecamere

2.8.2 Sistema centrale

2.8.3 Accesso alle immagini

2.9 Fototrappole

2.10 Drone

2.11 Dash cam

2.12 Body cam

3 Necessità e proporzionalità del trattamento

3.1 Legittimità

3.2 Liceità

3.3 Necessità

3.4 Limitazione della conservazione

3.5 Rapporti con gli interessati

3.5.1 Informative

3.5.2 Diritti degli interessati

4 Rischi per gli interessati e misure di contenimento

4.1 Metodologia

4.1.1 Minacce

4.1.2 Eventi

4.1.3 Stima del danno dell'evento (D)

4.1.4 Stima della probabilità dell'evento (P)

4.1.5 Valutazione del rischio di un evento (R)

4.2 Valutazione dei rischi e misure di contenimento

4.2.1 Minaccia zero

4.2.2 Minaccia interna

4.2.3 Minaccia esterna

5 Conclusioni

1 Introduzione

1.1 Oggetto e scopo

Il presente documento svolge la valutazione di impatto sulla protezione dei dati personali ai sensi degli articoli 35 e 36 del Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (nel seguito GDPR) per i sistemi di videosorveglianza (VSS) gestiti dal Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Siziano, mediante il sistema di videosorveglianza dei comuni di Pieve Emanuele e Siziano, integrato da un sistema di rilevamento e lettura delle targhe e dei transiti, attivati nel territorio urbano di detti comuni e collegato alla centrale operativa situata presso il Comando del Corpo Intercomunale di Polizia Locale sito nel comune di Pieve Emanuele.

1.2 Versione

Le misure tecniche ed organizzative per la protezione dei dati personali evolvono nel tempo in funzione dei miglioramenti tecnologici offerti dal mercato, delle nuove funzionalità richieste alla videosorveglianza, dei cambiamenti normativi che regolano la videosorveglianza (compresi gli interventi del Garante per la protezione dei dati personali e le Linee Guida europee) e delle nuove minacce portate ai sistemi dal mutato assetto politico – economico generale.

Il presente documento svolge la valutazione di impatto tenendo conto dello stato dell'arte al mese di agosto 2025.

1.3 La valutazione di impatto sulla protezione dei dati (DPIA)

L'art.35.1 GDPR prevede che "quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali".

Per gli scopi del presente documento, si evidenzia che l'art.35.3.c GDPR impone la valutazione d'impatto sulla protezione dei dati (DPIA) nel caso di "sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

L'art.35.7 GDPR elenca i contenuti obbligatori della DPIA:

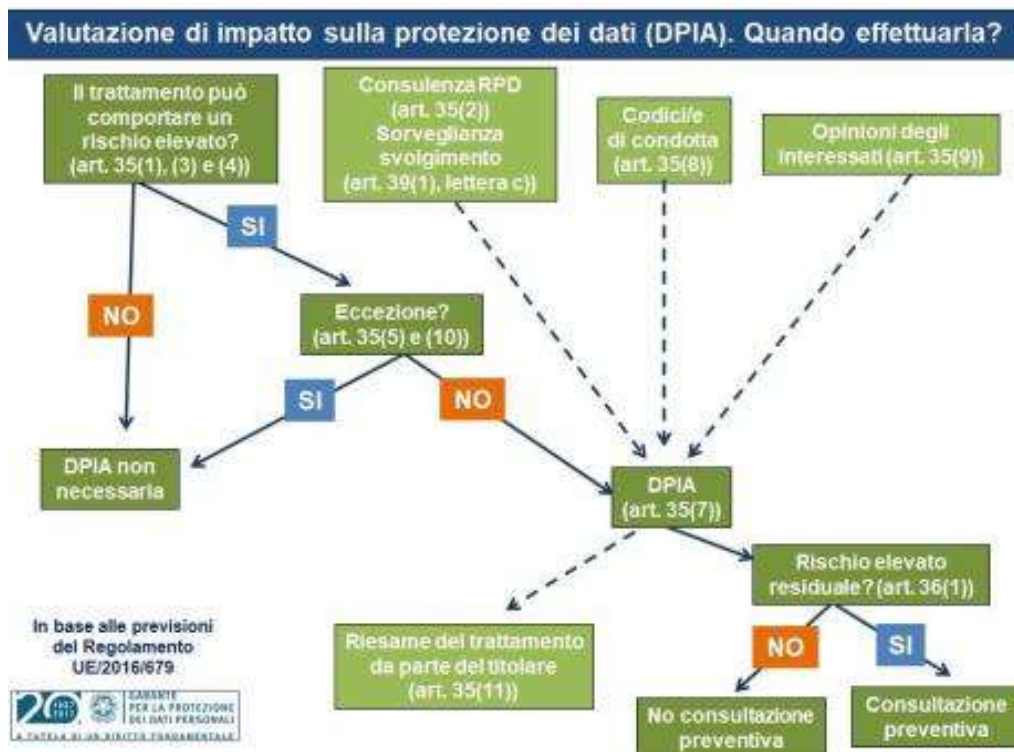
- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. L'art.36.1 GDPR richiede che "qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio" il titolare del trattamento, prima di procedere al trattamento, consulti l'Autorità di Controllo, che per l'Italia è il Garante per la Protezione dei Dati Personali (GPDP).

1.4 Le Linee Guida in materia di DPIA (LG-DPIA)

Le "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679" - WP 248 rev.01 del Gruppo di Lavoro Articolo 29 (*Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.*) per la protezione dei dati (LG-DPIA):

<https://ec.europa.eu/newsroom/article29/items/611236> forniscono indicazioni operative in materia di DPIA. In particolare, specificano il seguente processo di valutazione (*Lo schema del processo di valutazione qui riportato è la versione pubblicata nella sezione dedicata alla DPIA sul sito*

GPDP: <https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia->) che, partendo da una valutazione iniziale del rischio del trattamento, conduce o meno alla necessità di procedere alla DPIA (art.35 GDPR) e, nel caso in cui il trattamento riesaminato presenti ancora un rischio residuo elevato, alla consultazione preventiva presso il Garante (art.36 GDPR):



Per quanto riguarda la metodologia di valutazione, ricordato che il GDPR “offre ai titolari del trattamento la flessibilità di stabilire la struttura e la forma precise della valutazione d'impatto sulla protezione dei dati in maniera da consentire che la stessa si adatti alle pratiche di lavoro esistenti”, l’Allegato 2 delle LG-DPIA individuano i seguenti criteri comuni che, dettagliando i contenuti obbligatori indicati dall’art.35.7 GDPR, possono dimostrare che una particolare metodologia di valutazione soddisfa la norma:

Allegato 2 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- ☐ una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):
 - ☐ la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
 - ☐ vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
 - ☐ viene fornita una descrizione funzionale del trattamento;
 - ☐ sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
 - ☐ si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- ☐ la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):
 - ☐ sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
 - ☐ misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
 - ☐ finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
 - ☐ liceità del trattamento (articolo 6);
 - ☐ dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
 - ☐ limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
 - ☐ misure che contribuiscono ai diritti degli interessati:
 - ☐ informazioni fornite all'interessato (articoli 12, 13 e 14);
 - ☐ diritto di accesso e portabilità dei dati (articoli 15 e 20);
 - ☐ diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
 - ☐ diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
 - ☐ rapporti con i responsabili del trattamento (articolo 28);
 - ☐ garanzie riguardanti trattamenti internazionali (capo V);
 - ☐ consultazione preventiva (articolo 36).
- ☐ i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):
 - ☐ l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
 - ☐ si considerano le fonti di rischio (considerando 90);
 - ☐ sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
 - ☐ sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
 - ☐ sono stimate la probabilità e la gravità (considerando 90);
 - ☐ sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);
- ☐ le parti interessate sono coinvolte:
 - ☐ si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
 - ☐ si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).

Le LG-DPIA concludono che “spetta al titolare del trattamento scegliere una metodologia che, comunque, deve essere conforme ai criteri di cui all'allegato 2”.

1.5 Le Linee Guida sulla videosorveglianza (LG-VS)

Le “Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0” (LG-VS) adottate il 29 gennaio 2020 dal Comitato Europeo per la Protezione dei Dati (*Il Comitato Europeo per la Protezione dei Dati (EDPB)* è l'organizzazione sotto la cui egida si riuniscono le Autorità nazionali per la protezione dei dati personali dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati (EDPS). L'EDPB garantisce che il GDPR e la Direttiva “polizia e giustizia” siano applicati in modo coerente; inoltre, l'EDPB garantisce la cooperazione, anche in materia di attuazione della normativa. L'EDPB adotta decisioni vincolanti sui casi transfrontalieri sui quali non viene raggiunto un consenso) https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf mirano a fornire indicazioni sull'applicazione del GDPR nei trattamenti eseguiti coi VSS, inclusi quelli ritenuti necessari “allo scopo di eseguire un compito nell'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento” (paragrafo 3.2) come nel caso della videosorveglianza gestita dalla Polizia Locale.

Il paragrafo 9.3.1 LG-VS suggerisce che “oltre alla eventuale necessità di una DPIA, nell'elaborare le proprie politiche e procedure di videosorveglianza i titolari del trattamento dovrebbero prendere in considerazione” le seguenti misure organizzative:

- Responsabilità della gestione e del funzionamento del VSS.
- Finalità e ambito di applicazione del progetto di videosorveglianza.
- Utilizzo appropriato e vietato (dove e quando la videosorveglianza è consentita e dove e quando non lo è: ad esempio, uso di telecamere nascoste e registrazione audio oltre che video)
- Misure di trasparenza di cui alla sezione 7 (Obblighi di trasparenza e informazione)
- Modalità e durata delle registrazioni video, compresa la conservazione delle videoregistrazioni relative a problemi di sicurezza.
- Chi deve seguire una formazione specifica e quando.
- Chi ha accesso alle registrazioni video e per quali scopi.
- Procedure operative (ad esempio, da chi e da dove viene monitorata la videosorveglianza, cosa fare in caso di un problema di violazione dei dati).
- Quali procedure devono seguire i soggetti esterni per richiedere le videoregistrazioni e le procedure per respingere o accogliere tali richieste.
- Procedure per l'approvvigionamento, l'installazione e la manutenzione di VSS.
- Gestione dei problemi e procedure di recupero.

Il paragrafo 9.3.2 LG-VS fornisce alcuni elementi per le misure tecniche:

- Sicurezza fisica delle apparecchiature da furti, atti vandalici, calamità naturali, catastrofi provocate dall'uomo e danni accidentali
- Sicurezza del sistema e dei dati, cioè la protezione da interferenze volontarie e involontarie nel suo normale funzionamento, che include:
 - protezione dell'intera infrastruttura (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni fisiche e furti;
 - protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione;
 - cifratura dei dati;
 - utilizzo di soluzioni basate su hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;
 - rilevamento di guasti di componenti, software e interconnessioni;
 - strumenti per ripristinare la disponibilità dei dati personali e l'accesso agli stessi in caso di problemi fisici o tecnici.
- Controllo degli accessi a garanzia che solo le persone autorizzate possano accedere al sistema e ai dati, che include:

- la garanzia che tutti i locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in cui vengono conservate le riprese video siano protetti contro l'accesso non supervisionato da parte di terzi;
- il posizionamento dei monitor (soprattutto quando si trovano in zone aperte, come una reception) in modo tale che solo gli operatori autorizzati possano visualizzarli;
- la definizione e l'applicazione delle procedure per la concessione, la modifica e la revoca dell'accesso;
- l'attuazione di metodi e mezzi di autenticazione e autorizzazione dell'utente, tra cui ad esempio la lunghezza delle password e la frequenza della loro modifica;
- la registrazione e la revisione periodica delle azioni eseguite dagli utenti (con riguardo sia al sistema sia ai dati);
- l'esecuzione del monitoraggio e l'individuazione di guasti agli accessi in modo continuativo e la risoluzione in tempi brevi delle carenze individuate.

1.6 Obbligatorietà della DPIA per la videosorveglianza della Polizia Locale

Per le sue finalità e per le sue caratteristiche tecniche, i VSS della Polizia Locale dell'Ente sono in grado di attuare una "sorveglianza sistematica su larga scala di zone accessibili al pubblico" ai sensi dell'art.35 GDPR. Si ritiene quindi che i trattamenti sui dati personali svolti da tali sistemi richiedano la DPIA, svolta nei capitoli che seguono del presente documento.

Alla data del presente documento, non risulta che GPDP abbia reso pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati (art.35.5 GDPR) né risulta che si sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione della normativa che regola la videosorveglianza della Polizia Locale (art 35.10 GDPR). Non si applicano quindi le eccezioni previste dal processo di valutazione che consentirebbero di non procedere alla DPIA.

1.7 Struttura della DPIA e sua conformità al GDPR

La DPIA svolta nel presente documento è strutturata in capitoli che rispondono positivamente ai contenuti richiesti dall'art.35.7 GDPR ed alle raccomandazioni contenute nelle LG-DPIA e LG-VS, nonché alla valutazione finale richiesta dall'art.36.1 GDPR:

Art. GDPR	Requisito	Descritto nel capitolo del presente documento
35.7.a	descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento	1 e 2
35.7.b	valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità	3
35.7.c	valutazione dei rischi per i diritti e le libertà degli interessati	4
35.7.d	misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione	
36.1	Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio	5

1.8 Abbreviazioni

CPDP	D.Lgs. 196/2003 Codice in materia di protezione dei dati personali
DPIA	Data Protection Impact Analysis: Valutazione di impatto sulla protezione dei dati (art.35 GDPR)
GDPR	General Data Protection Regulation: Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016
GPDP	Garante per la Protezione dei Dati Personali ("Garante Privacy" italiano)
LG-DPIA	Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679 - WP 248 rev.01 del Gruppo di Lavoro Articolo 29 per la protezione dei dati
LG-VS	Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video – Versione 2.0, adottate il 29 gennaio 2020 dal Comitato Europeo per la Protezione dei Dati
RCVS	"Regolamento per la disciplina della videosorveglianza", approvato con deliberazione di Consiglio Comunale del comune di Pieve Emanuele n. 34/2021 e deliberazione di Consiglio Comunale del comune di Siziano n. 9/2022
RPD	Responsabile della Protezione dei Dati (art.37 e seguenti GDPR)
VSS	Sistemi di videosorveglianza
WSUS	Windows Server Update Services: sistema software per la distribuzione degli aggiornamenti dei prodotti Microsoft

2 Descrizione del trattamento

Il presente capitolo descrive il trattamento svolto coi VSS dal Corpo Intercomunale di Polizia Locale dei Comuni di Pieve Emanuele e Siziano, fornendo i necessari elementi conoscitivi relativi alla finalità ed ai mezzi del trattamento.

2.1 Contesto e finalità

2.1.1 Il Regolamento comunale per l'utilizzo di impianti di videosorveglianza (RCVS)

Con deliberazione di Consiglio Comunale n. 34/2021, il Comune di Pieve Emanuele ha approvato il "Regolamento per la disciplina della videosorveglianza del comune di Pieve Emanuele" (RCVS), pubblicato sul sito istituzionale dell'Ente:

https://www.comune.pieveemanuele.mi.it/it/documenti_pubblici/regolamento-videosorveglianza-2021.

Con deliberazione di Consiglio Comunale n. 9/2022, il Comune di Siziano ha approvato, gli Enti ha approvato il "Regolamento per la disciplina della videosorveglianza del comune di Siziano" (RCVS), pubblicato sul sito istituzionale dell'Ente:

https://www.comune.siziano.pv.it/documento_pubblico/regolamento-videosorveglianza/.

L'art. 4 del RCVS definisce le seguenti finalità per la videosorveglianza e quindi per i trattamenti svolti attraverso di esso:

- prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del decreto legge n. 14/2017 e delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art. 50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del d.lgs 267/2000;*
- prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado e abbandono di rifiuti, e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nel regolamento di Polizia Urbana, nei regolamenti locali in genere e nelle ordinanze sindacali;*
- vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;*
- tutelare l'ordine, il decoro e la quiete pubblica;*

- e) *controllare aree specifiche del territorio comunale;*
- f) *identificare, in tempo reale, di criticità viabilistiche in modo tale da poter predisporre un tempestivo intervento degli organi di Polizia Stradale;*
- g) *rilevare dati anonimi o pseudonimizzati per l'analisi dei flussi di traffico e per la predisposizione di piani comunali del traffico;*
- h) *verificare la funzionalità degli impianti semaforici;*
- i) *attivare uno strumento operativo di protezione civile sul territorio comunale;*
- j) *acquisire fonti di prova in caso di illeciti penali o atti di accertamento in caso di violazioni amministrative.*

2.2 Ciclo di vita dei dati personali trattati

Al di là delle differenze tecniche dei diversi VSS, il ciclo di vita dei dati personali trattati con i VSS è così descrivibile. Si rinvia all'art. 12 RCVS e alle sezioni seguenti del presente documento per i dettagli.



2.2.1 Raccolta

I dati personali sono raccolti mediante telecamere digitali fisse e mobili, con diverse funzionalità (es. brandeggio e zoom, riconoscimento automatico di numeri e cifre delle targhe) e capacità (es. risoluzione, infrarosso, identificazione del movimento).

2.2.2 Trasmissione

I dati sono trasmessi in forma crittografica mediante network dedicato che collega i dispositivi di raccolta direttamente ai sistemi server della videosorveglianza di pertinenza. Il network dati non è in collegamento con altri servizi/funzioni comunali.

Alcune tipologie di telecamere mobili non trasmettono le immagini, ma le registrano su memoria locale rimovibili, dalle quali gli operatori provvedono a scaricare i dati sui sistemi centrali.

2.2.3 Elaborazione e visualizzazione

Le immagini sono archiviate su sistemi centrali gestiti dal Corpo Intercomunale di Polizia Locale e sono visualizzate in tempo reale o differito su monitor collocati nella Sala Operativa e quindi visibili solo ai soggetti autorizzati. L'archiviazione è necessaria per consentire la visualizzazione differita, ad esempio per la documentazione di un evento avvenuto mentre la Sala Operativa non è presidiata. Le password di accesso hanno scadenza e che sono aggiornate mediamente semestralmente. Per variazione di ruolo/funzione dei soggetti autorizzati, la gestione centrale degli Utenti permette di sospendere o cancellare in tempo reale qualsiasi permissione di accesso a sistema.

2.2.4 Distribuzione

Nel caso in cui gli organi della Polizia dello Stato o della Polizia locale, nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate che sono contenute nelle riprese effettuate, possono farne richiesta scritta e motivata indirizzata al RI. Gli artt. 14 e 17 RCVS regolano la comunicazione delle immagini a terzi.

2.2.5 Conservazione e cancellazione

Il termine massimo di durata della conservazione dei dati è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di VSS, fatte salve speciali esigenze di ulteriore conservazione (art. 12 RCVS), ad esempio su specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria in relazione ad una attività investigativa in corso (art. 12 RCVS), così come disciplinato dal DPR

15/2018 e dal D. Lgs. 51/2018. La conservazione avviene su 5 Server di differente tipologia, muniti di sistema operativo Windows Server da versione 2019 in avanti, regolarmente mantenuto aggiornato, di cui 3 posizionati presso la sede del Comando del Corpo Intercomunale (in apposito locale chiuso a chiave e dotato di impianto di climatizzazione), 1 posto presso gli uffici del Distaccamento di Siziano del Corpo Intercomunale (in armadio chiuso a chiave) e il quinto dislocato presso il municipio di Pieve Emanuele (in apposito locale chiuso a chiave). Copia di sicurezza con procedura automatica, effettuata su infrastruttura secondaria, nello stesso locale del Comando, protetto e non accessibile al pubblico.

I dati raccolti con gli impianti di foto sorveglianza e videosorveglianza mobili (Art. 1 c. 5 RCVS) sono trasferiti su di un portale informatico in dotazione alla Centrale Operativa del Corpo Intercomunale. Il trasferimento di dati da tali strumenti alla struttura informatica della Centrale Operativa del Corpo Intercomunale avviene manualmente senza collegamenti con altri sistemi o con altre reti pubbliche di telecomunicazioni, né attraverso l'accesso di altre periferiche ed è effettuato dal designato o dai preposti, muniti di credenziali di accesso (nome utente e password). Il Trasferimento dei dati dalle body cam (Art. 13 RCVS) alla struttura informatica della Centrale Operativa del Corpo Intercomunale avviene automaticamente (non vi è alcuna possibilità di modificare, cancellare e/o svolgere alcuna funzione) inserendo la body cam nell'apposito slot. Una volta scaricato nel sistema centrale il video diviene disponibile come se provenisse da una delle telecamere fisse.

Per quanto concerne l'utilizzo dei dati ai fini della contestazione degli illeciti amministrativi, gli stessi verranno conservati per il solo tempo strettamente necessario in riferimento: alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'Autorità Giudiziaria o di Polizia Giudiziaria.

2.3 Misure organizzative

Il CAPO IV del RCVS descrive l'organizzazione predisposta per la protezione dei dati personali trattati con i VSS, qui integrata con informazioni relative all'organizzazione generale per la protezione dei dati personali dell'Ente.

2.3.1 Titolare del trattamento

Il Titolare del trattamento effettuato con l'impianto di videosorveglianza del Corpo Intercomunale è:
per il comune di Pieve Emanuele: il Comune di Pieve Emanuele, P.I. 04239310156, c.f. 80104290152, con sede in Pieve Emanuele (MI), via Viquarterio 1, nella figura del Sindaco quale rappresentante legale dell'Ente;
per il comune di Siziano: il Comune di Siziano, c.f. e P.IVA. 00478370182, con sede in Siziano (PV), piazza G. Negri 1, nella figura del Sindaco quale rappresentante legale dell'Ente.

2.3.2 Responsabile della Protezione dei Dati

Il Titolare ha provveduto a designare un Responsabile della Protezione dei Dati (Art. 9 RCVS) ai sensi dell'art. 37 e ss. GDPR.

2.3.3 Soggetti autorizzati

Ai sensi dell'art. 29 GDPR e dell'art. 2-quaterdecies comma 2 CPDP, RPD designa come soggetti autorizzati (Art. 10 RCVS) tutte le persone fisiche autorizzate al materiale trattamento dei dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Titolare o del Responsabile, utilizzando gli impianti nei casi in cui sia indispensabile per gli scopi perseguiti.

Il numero di soggetti autorizzati è delimitato e sufficiente a garantire la gestione del servizio di videosorveglianza nell'ambito degli operatori di Polizia Locale.

Il PPD provvede ad individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo soggetto autorizzato, che deve essere in possesso di credenziali di autenticazione che permettono di effettuare a seconda dei compiti attribuiti unicamente le operazioni di propria competenza, distinguendo coloro che sono unicamente abilitati a visionare le immagini, dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni quali la registrazione, la copia, la cancellazione, la modifica dello zoom, etc.

In occasione degli aggiornamenti apportati ai VSS, i soggetti autorizzati ricevono istruzioni mediante formazione.

Il Titolare vigila, anche tramite verifiche periodiche, l'osservazione delle disposizioni da parte del Responsabile interno e dei soggetti autorizzati.

2.3.4 Responsabili esterni

Ai sensi dell'art. 28 GDPR, il Titolare designa quale Responsabili esterni del trattamento (Art. 11 RCVS) i soggetti esterni incaricati per contratto della installazione o manutenzione dell'impianto di videosorveglianza. I trattamenti effettuati dai Responsabili Esterni sono disciplinati nel contratto o con atto separato, che regola anche l'eventuale autorizzazione da parte del Titolare a ricorrere ad altro responsabile (sub fornitore) in via generale o specifica ai sensi dell'art. 28.2 GDPR.

2.3.5 Amministratori di Sistema

Ai sensi del Provvedimento GPD del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", il Titolare o RPD designano uno o più Amministratori di Sistema, tenendo conto della molteplicità delle tecnologie utilizzate nei diversi VSS.

2.3.6 Registro dei trattamenti

Ai sensi dell'art.30 GDPR, il Titolare tiene un Registro delle attività di trattamento che include le attività di trattamento effettuate con i VSS.

2.4 Tipologie di VSS in utilizzo

Presso il Corpo Intercomunale di Polizia Locale sono in utilizzo diversi VSS, distinti per funzionalità ed architettura (Art. 1, Art. 13 RCVS), nel seguito sinteticamente descritti:

- una rete di telecamere fisse a colori per la videosorveglianza del territorio;
- una rete di telecamere di lettura e riconoscimento targhe, certificate secondo UNI 10772:2016. I fotogrammi delle targhe sono contraddistinti da inclusione automatica di certificato digitale SHA-2 univoco che ne garantisce l'originalità specificando, tra l'altro, il numero di matricola del dispositivo di provenienza e l'impossibilità di manipolazione. I dispositivi sono collocati sulle principali arterie di entrata ed uscita dai territori dei comuni di Pieve Emanuele e Siziano;
- telecamere mobili per lettura e riconoscimento targhe posizionate su veicoli di servizio della Polizia Locale;
- telecamere per controllo infrazioni passaggio con semaforo rosso;
- fototrappole per vigilanza sui rifiuti e finalità di Polizia Giudiziaria;
- drone per attività di controllo del territorio, prevenzione di illeciti amministrativi o reati, monitoraggio del traffico, ricerca di persone scomparse, attività di Polizia Amministrativa e/o Polizia Giudiziaria
- Dash cam, installate sui veicoli di servizio della Polizia Locale per registrare gli eventi che accadono all'esterno dell'autovettura nella direzione in cui sono rivolte;
- Body cam, telecamere indossabili, destinate alla videoripresa durante il servizio degli Operatori di Polizia Locale addetti alla sicurezza e al controllo del territorio.

L'elenco per tipologia e numero dei dispositivi utilizzati nei diversi VSS e le corrispondenti schede tecniche sono conservati da RPD.

2.5 Videosorveglianza del territorio

Il VSS dedicato alla videosorveglianza dei Comuni di Pieve Emanuele e Siziano è costituito da 52 gruppi di telecamere (29 gruppi a Pieve Emanuele e 23 Gruppi a Siziano), cui sono collegate in totale 229 flussi video telecamere (152 a Pieve Emanuele e 76 a Siziano).

2.5.1 Telecamere

Le telecamere inquadrano piazze, parcheggi, parchi, accessi principali alla città e vie in cui sono presenti servizi pubblici quali scuole, impianti sportivi, farmacie, cimiteri, parchi, stazioni ferroviarie, parcheggi. Una minima parte delle telecamere sono motorizzate (dome), consentendo quindi operazioni di brandeggio e zoom. La trasmissione delle riprese dalle telecamere al sistema centrale di elaborazione ed archiviazione è realizzata con ponti radio 5 Ghz, protetta da cifratura WPA2, di proprietà dell'Ente. Le telecamere sono fisicamente posizionate in modo da rendere molto difficile il raggiungimento delle stesse. Appositi armadi di contenimento dei sottosistemi sono concepiti per protezione antivandalo, con chiusura a chiave, anch'essi posizionati in modo da risultare molto difficilmente raggiungibili se non con apposite scale o mezzi di sollevamento.

2.5.2 Sistema centrale

Il sistema centrale è ospitato nella sala server presso il Comando del Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Siziano dotato di accesso controllato, impianto antifurto, impianto di climatizzazione, impianto di allarme antincendio e presidi antincendio. L'accesso al sistema centrale dall'esterno è protetto da firewall, su cui è attivo un contratto di manutenzione e gestione.

Sul sistema sono in essere ridondanze hardware dei componenti critici e sono attuati con scadenza definite gli aggiornamenti del sistema operativo e degli applicativi in uso. I sistemi si contraddistinguono da elevati standard tecnologici e includono il LOG degli accessi attuati da parte degli Operatori e i LOG di auto diagnosi delle telecamere connesse.

2.5.3 Accesso alle immagini

Ai sensi dell'art.7 DPR 15/2018 "l'uso, anche per finalità di analisi, di particolari tecniche di elaborazione delle informazioni, ivi inclusi i sistemi di indice, è consentito ai soli operatori a ciò abilitati e designati, secondo profili di autorizzazione predefiniti in base alle indicazioni del capo dell'ufficio o del comandante del reparto e nell'ambito di specifiche attività informative, di sicurezza o di indagine di polizia giudiziaria".

L'accesso al sistema avviene attraverso credenziali locali. I soggetti autorizzati non operano con privilegi di amministratore.

La visualizzazione in tempo reale delle riprese effettuate dalle telecamere avviene su schermi collocati presso la Sala Operativa del Comando del Corpo Intercomunale di Polizia Locale. La Sala Operativa non è accessibile al pubblico e non è possibile visionare lo schermo dall'esterno.

Le riprese sono visualizzate in differita su autorizzazione del Responsabile interno.

Esiste un Registro degli accessi, in cui gli operatori dichiarano la motivazione per l'accesso alle immagini registrate nel sistema.

2.6 Lettura targhe

Il sistema è costituito da una rete di 38 telecamere (17 a Pieve Emanuele e 21 a Siziano) per la lettura e riconoscimento delle targhe veicolari Europee e sono conformi a certificazione UNI 10772:2016. I dispositivi sono posti sulle principali arterie di entrata ed uscita dai territori dei comuni di Pieve Emanuele e Siziano a supporto dei controlli previsti dal Codice della Strada (copertura assicurativa, revisione, ecc.), controlli ambientali (classe Euro) nonché per attività di Polizia Giudiziaria.

L'accesso a qualsiasi dispositivo del sistema è subordinato a inserimento di user e password specifica.

2.6.1 Telecamere

La trasmissione delle riprese dalle telecamere al sistema centrale di elaborazione ed archiviazione è realizzata con ponti radio 5 Ghz, protetta da cifratura WPA2, di proprietà dell'Ente. Il network è esclusivo e segmentato per zona, con una gestione di tele diagnostica automatica.

L'accesso a qualsiasi dispositivo di trasmissione dati è subordinato a inserimento di user e password specifica.

2.6.2 Sistema centrale

Il sistema centrale è ospitato nella sala server presso il Comando del Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Sizzano dotato di accesso controllato, impianto antifurto, impianto di climatizzazione, impianto di allarme antincendio e presidi antincendio. L'accesso al sistema centrale dall'esterno è protetto da firewall, su cui è attivo un contratto di manutenzione e gestione.

I Server sono basati su ambiente operativo Microsoft Windows Server da versione 2019 in avanti. Attive tutte le policy di sicurezza di riferimento. L'accesso ai server della video sorveglianza è protetto da password.

2.6.3 Accesso alle immagini

La visualizzazione delle immagini avviene per la verifica da parte dell'Operatore del numero di targa identificato automaticamente dal sistema ai fini del controllo di polizia stradale, oppure inserendo il numero di targa ricercato per attività di Polizia Giudiziaria.

2.7 Telecamere mobili per lettura targhe

Il Corpo Intercomunale di Polizia Locale è dotato di 2 telecamere mobili per lettura targhe, utilizzate con le medesime finalità indicate al punto 2.6. Gli operatori non hanno alcun modo di accedere materialmente ai dispositivi la cui gestione, manutenzione e aggiornamento è in capo alla ditta incaricata all'assistenza tecnica.

2.7.1 Telecamere

Tali telecamere vengono installate a bordo dei veicoli di servizio della Polizia Locale collegate tramite router portatile al CED della Motorizzazione Civile per attuare controlli. L'accesso alle funzioni software avviene previo inserimento di password di accesso al dispositivo Tablet, successivo collegamento a VPN MCTC inserendo le necessarie credenziali di collegamento e password per accesso a banca dati.

I dati sono salvati sul Tablet e riversati manualmente a fine attività di pattugliamento senza collegamenti con altri sistemi o con altre reti pubbliche di telecomunicazioni, né attraverso l'accesso di altre periferiche. L'attività è effettuata dal designato o dai preposti muniti di specifiche credenziali di accesso (nome utente e password).

2.7.2 Accesso alle immagini

La visualizzazione delle immagini avviene per la verifica da parte dell'Operatore del numero di targa identificato automaticamente dal sistema ai fini del controllo di polizia stradale e/o polizia giudiziaria.

2.8 Telecamere controllo infrazioni passaggio con semaforo rosso

Su un impianto semaforico situato nel comune di Pieve Emanuele, sono installate 2 dispositivi approvati dal MIT per il controllo delle infrazioni al passaggio con semaforo rosso. I dati rilevati in questi sistemi rimangono memorizzati localmente e sono trasferiti mediante procedura manuale mediante attivazione di collegamento VPN apposito e avvio della procedura di sincronizzazione/scarico rilievi. I dati dei rilievi sono visionati e trattati col programma di gestione dei sistemi installato in postazione di lavoro collocata presso gli uffici della Polizia Locale. I dati rilevati considerati validi sono vagliati e poi esportati manualmente nel separato programma di gestione C.d.S. Gli operatori non hanno alcun modo di accedere materialmente ai dispositivi di rilevamento infrazioni, essi sono ad esclusiva gestione da parte della ditta incaricata all'assistenza tecnica, manutenzione e aggiornamento.

2.8.1 Telecamere

La trasmissione dei rilevamenti al sistema centrale di elaborazione ed archiviazione dati è realizzata mediante connessione cellulare dedicata mediante SIM DATI.

2.8.2 Sistema centrale

Il sistema centrale è ospitato nella sala server presso il Comando del Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Siziano dotato di accesso controllato, impianto antifurto, impianto di climatizzazione, impianto di allarme antincendio e presidi antincendio. L'accesso al sistema centrale dall'esterno è protetto da firewall, su cui è attivo un contratto di manutenzione e gestione.

I Server sono basati su ambiente operativo Microsoft Windows Server da versione 2019 in avanti. Attive tutte le policy di sicurezza di riferimento. L'accesso ai server della video sorveglianza è protetto da password.

2.8.3 Accesso alle immagini

La visualizzazione delle immagini avviene per la verifica da parte dell'Operatore del numero di targa identificato automaticamente dal sistema ai fini del controllo di polizia stradale e/o polizia giudiziaria.

2.9 Fototrappole

Il Corpo Intercomunale di Polizia Locale è dotato di 22 fototrappole (15 Pieve Emanuele e 7 Siziano) utilizzate per diversi scopi, tra cui attività di polizia giudiziaria e repressione delle violazioni alle normative ambientali (sia amministrative che penali). L'accesso al dispositivo avviene attraverso l'inserimento di codice PIN. Le stesse vengono ancorate con catene e lucchetti per contenere il rischio di asportazione/furto.

2.10 Drone

Il Corpo Intercomunale di Polizia Locale è dotato di 1 drone utilizzato per attività di controllo del territorio, prevenzione di illeciti amministrativi o reati, monitoraggio del traffico, ricerca di persone scomparse, attività di protezione civile, attività di Polizia Amministrativa e/o Polizia Giudiziaria. L'utilizzo del drone è consentito solo agli Operatori in possesso dell'attestato di pilota APR.

2.11 Dash cam

Il Corpo Intercomunale di Polizia Locale è dotato di 5 dash cam installate sui veicoli di servizio per registrare gli eventi che accadono all'esterno dell'autovettura nella direzione in cui sono rivolte. L'accesso alle immagini avviene solamente se l'evento registrato ha rilevanza per attività di Polizia Amministrativa e/o Polizia Giudiziaria.

2.12 Body cam

Il Corpo Intercomunale di Polizia Locale è dotato di 15 body cam, telecamere indossabili, destinate alla videoripresa durante il servizio degli Operatori di Polizia Locale addetti alla sicurezza e al controllo del territorio. Ogni Body cam è assegnata ad ogni Operatore. L'accesso alle immagini avviene solamente se l'evento registrato ha rilevanza per attività di Polizia Amministrativa e/o Polizia Giudiziaria. I dispositivi sono conformi a norma sulla cybersecurity secondo direttiva ETSI EN 303645, etichetta di sicurezza BSI IT.

3 Necessità e proporzionalità del trattamento

Il presente capitolo fornisce gli elementi utili a valutare la necessità e la proporzionalità del trattamento effettuato coi VSS del Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Siziano, verificando quanto richiesto dalle LG-DPIA.

3.1 Legittimità

Il trattamento effettuato coi VSS da parte Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Siziano trova legittimità nella legislazione nazionale vigente, che attribuisce ai Comuni un ruolo di tutela della sicurezza urbana. In particolare, il D.L. 11/2019 all'art.6.7 sancisce che "Per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico". Altre norme di riferimento sono già state citate nel testo.

I trattamenti di dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali sono specificamente regolamentati dalla Direttiva (UE) 2016/680, recepita in Italia dal D. Lgs. 51/2018.

3.2 Liceità

La liceità di un trattamento deve trovare riscontro in una o più delle basi giuridiche previste dall'art.6 GDPR. Per il trattamento effettuato coi VSS da parte del Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Siziano, si identifica come base giuridica quella indicata alla lettera "e" dell'art.6.1 GDPR e cioè "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".

3.3 Necessità

Sia il Recital 39 (Considerando 39) del GDPR che il Recital 26 (Considerando 26) della succitata Direttiva 2016/680 ricordano che "i dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi".

Questa indicazione è puntualmente applicata al caso della videosorveglianza dal punto 3.1.2 LG-VS: "Prima di installare un sistema di videosorveglianza, il titolare del trattamento deve sempre valutare criticamente se questa misura sia in primo luogo idonea a raggiungere l'obiettivo desiderato e, in secondo luogo, adeguata e necessaria per i suoi scopi. Si dovrebbe optare per misure di videosorveglianza unicamente se la finalità del trattamento non può ragionevolmente essere raggiunta con altri mezzi meno intrusivi per i diritti e le libertà fondamentali dell'interessato."

Il medesimo principio di necessità è presente nel Provvedimento GDPR dell'8 aprile 2010 [doc - web 1712680]: l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure. <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1712680>

Il ricorso ai diversi VSS da parte del Corpo Intercomunale di Polizia Locale dei comuni di Pieve Emanuele e Siziano è giustificato dalla impossibilità a raggiungere le finalità di sicurezza urbana, di controllo dei mezzi circolanti, di monitoraggio del traffico, di polizia giudiziaria e di protezione degli agenti senza l'uso della videosorveglianza.

Si evidenzia inoltre che l'attuale numero di agenti incardinati nel Corpo (16) è inferiore al rapporto considerato ottimale di 1 Agente ogni 1.000 abitanti, considerando che il numero di abitanti del territorio servito è di oltre 22.000 abitanti.

3.4 Limitazione della conservazione

La conservazione dei dati provenienti dai VSS è attuata in conformità dell'art.6.8 D.L. 11/2019: "La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione".

3.5 Rapporti con gli interessati

Le LG-VS al punto 7 evidenziano che "La normativa europea in materia di protezione dei dati dispone da tempo che gli interessati debbano essere consapevoli del fatto che è in funzione un sistema di videosorveglianza. Dovrebbero essere informati in modo dettagliato sui luoghi sorvegliati" e prevedono per la videosorveglianza due livelli di informativa ex art. 13 GDPR: una segnaletica di avvertimento (primo livello) e una informativa completa (secondo livello).

3.5.1 Informative

Gli interessati sono informati attraverso una segnaletica di avvertimento conforme alle indicazioni delle LG-VS (informativa "breve") collocata nelle zone sottoposte a videosorveglianza, che rimanda alla informativa completa pubblicata sul sito istituzionale dell'Ente.

La segnaletica di avvertimento è collocata anche nel caso di utilizzo di VSS mobile per il controllo di situazione si degrado quali l'abbandono di rifiuti.

3.5.2 Diritti degli interessati

Agli interessati di cui sono riprese le immagini dai VSS sono riconosciuti i diritti di cui agli art. 14 RCSV, 14 e seguenti GDPR, con alcune limitazioni discendenti dalle finalità, della base giuridica e delle caratteristiche specifiche del trattamento di videosorveglianza ed in particolare:

- diritto di accesso ai propri dati personali (art.15 GDPR) secondo quanto previsto dall'art.24 L. 241/90 ("accesso documentale" - Si veda ad esempio TAR Puglia, sez. II, 2 novembre 2021, n. 1579);
- diritto di rettifica dei dati personali inesatti (art.16 GDPR) es. nel caso di errata identificazione dell'interessato a partire dai dati di targa del veicolo letti automaticamente dal sistema;
- diritto alla cancellazione (art.17 GDPR) non è esercitabile perché il Titolare esegue il trattamento nell'esercizio di pubblico potere (art.17.3.b GDPR);
- diritto di limitazione di trattamento (art.18 GDPR);
- obbligo di notifica in caso di rettifica o cancellazione dei dati o limitazione del trattamento (art.19 GDPR)
- diritto alla portabilità (art.20 GDPR) non è esercitabile perché il Titolare esegue il trattamento nell'esercizio di pubblico potere (art.20.3 GDPR);
- diritto di opposizione al trattamento (art.21 GDPR) non è esercitabile perché il Titolare esegue il trattamento per compito di interesse pubblico (art 21.6 GDPR);
- diritto di non essere sottoposto ad un processo decisionale automatizzato (art.22 GDPR) non trova attualmente applicazione in quanto la Polizia Locale non assume decisioni unicamente basati sul trattamento automatizzato (es. la targa letta automaticamente viene controllata visivamente dall'operatore prima dell'emissione della sanzione).

4 Rischi per gli interessati e misure di contenimento

Questo capitolo svolge la valutazione dei rischi per i diritti e le libertà degli interessati, derivanti da violazioni di riservatezza, integrità e disponibilità dei dati personali trattati nei VSS alla luce delle misure tecniche ed organizzative di contenimento del rischio predisposte o in via di attuazione.

4.1 Metodologia

Per la valutazione dei rischi si adotta la seguente metodologia.

4.1.1 Minacce

La valutazione dei rischi è eseguita a fronte delle seguenti minacce:

Minaccia	Descrizione
Zero	I VSS sono utilizzati solo dai soggetti autorizzati, che seguono le istruzioni loro impartite; questa minaccia consente di valutare il rischio base insito nei VSS per così come sono realizzati, a prescindere da comportamenti malevoli da parte di utenti o di terzi.
Interna	I VSS sono utilizzati dai soggetti autorizzati che non seguono le istruzioni loro impartite; questa minaccia consente di valutare il rischio aggiuntivo apportato da un comportamento non adeguato dei soggetti autorizzati e non impedito dalle protezioni "fin dalla progettazione e per impostazione predefinita" (art.25 GDPR) presenti nei VSS.
Esterna	I VSS sono utilizzati da soggetti non autorizzati, attraverso azioni tese a superare le protezioni presenti nei VSS.

4.1.2 Eventi

Per ogni minaccia, si identificano eventi verosimili (cioè con probabilità non completamente trascurabile) che possono comportare danni agli interessati, considerando le tre principali componenti tecnologiche dei SDV (telecamere, connessioni di trasmissione, elaboratori centrali) e le tre tipologie di violazioni (riservatezza, integrità, disponibilità).

4.1.3 Stima del danno dell'evento (D)

Il danno ai diritti e le libertà dell'interessato conseguente all'accadimento di un evento è valutato utilizzando la seguente scala discreta di valori:

Livello	Valore	Descrizione
1	Disagio minore	Gli interessati possono andare incontro a disagi minori, che supereranno senza conseguenze di lungo periodo (perdita di tempo, rinvio di un servizio, irritazione...)
2	Disagio maggiore	Gli interessati possono andare incontro a significativi disagi, che supereranno con alcune difficoltà (costi aggiuntivi, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità...)
3	Danno superabile	Gli interessati possono andare incontro a conseguenze significative ai loro diritti e libertà individuali, che dovrebbero essere in grado di superare anche se con gravi difficoltà (perdite di denaro, danni di reputazione, danni alla proprietà, perdita del lavoro, citazione in giudizio, peggioramento della salute...)
4	Danno insuperabile	Gli interessati possono subire conseguenze significative o irreversibili ai loro diritti e libertà individuali, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte...)

4.1.4 Stima della probabilità dell'evento (P)

La probabilità di accadimento di un evento è valutata utilizzando la seguente scala discreta di valori:

Livello	Valore	Descrizione
1	Improbabile	Non risulta che l'evento sia mai capitato ed il suo accadimento sorprenderebbe molto
2	Occasionale	Non si può escludere che l'evento sia accaduto in passato e che possa accadere in futuro
3	Probabile	L'evento è già accaduto in passato e/o se accadesse in futuro non sorprenderebbe
4	Frequente	L'evento è già accaduto più volte

4.1.5 Valutazione del rischio di un evento (R)

Il rischio è valutato sulla base delle stime di danno e probabilità utilizzando la seguente tabella di calcolo:

4 Danno insuperabile	4 Medio	8 Alto	12 Elevato	16 Elevato
3 Danno superabile	3 Medio	6 Alto	9 Alto	12 Elevato
2 Disagio maggiore	2 Basso	4 Medio	6 Alto	8 Alto
1 Disagio minore	1 Basso	2 Basso	3 Medio	4 Medio
	1 Improbabile	2 Occasionale	3 Probabile	4 Frequente

La tabella definisce quattro possibili livelli di rischio:

Livello	Valore	Conseguenze
1-2	Basso	Il rischio è accettabile
3-4	Medio	Il rischio è accettabile e si raccomanda la ricerca ed esecuzione di ulteriori misure di riduzione
6-9	Alto	Il rischio è accettabile solo nel breve – medio periodo e deve essere affrontato con ulteriori misure di riduzione
12-16	Elevato	Il rischio richiede l'applicazione dell'art.36 GDPR.

4.2 Valutazione dei rischi e misure di contenimento

Utilizzando la metodologia precedentemente descritta, in questa sezione si procede alla valutazione del rischio per ogni minaccia/componente/violazione.

4.2.1 Minaccia zero

Componente	Violazione	Evento	D	P	R	Nota e Misure di contenimento
Telecamere*	Riservatezza	Nessun evento particolare identificato	1	1	1	Le telecamere sono asservite ai sistemi di elaborazione e non sono in grado di comunicare autonomamente con altri sistemi
Telecamere*	Integrità	Errata lettura automatica della targa	2	1	2	L'emissione della sanzione avviene solo dopo verifica della immagine da parte dell'incaricato
Telecamere*	Disponibilità	Mancato funzionamento telecamera	1	2	2	La probabilità che sia guasta proprio la telecamera di interesse è valutata bassa per la numerosità delle telecamere e l'attivazione di un contratto di manutenzione/sostituzione
Conessioni	Riservatezza	Errata configurazione della connessione	2	1	2	L'installazione e la configurazione sono effettuate da società specializzate
Conessioni	Integrità	Disturbi sulle comunicazioni	2	1	2	I protocolli di comunicazione correggono gli errori di trasmissione
Conessioni	Disponibilità	Interruzione accidentale del ponte radio	2	1	2	Attivo servizio di pronto intervento per riparazione guasto
laboratori	Riservatezza	Accesso da parte di ex incaricati	3	1	3	Le credenziali vengono revocate alla cessazione del rapporto di lavoro.
Elaboratori	Integrità	Errata profilazione degli utenti o mancato aggiornamento delle profilazioni rilasciate	3	1	3	Autorizzazione scritta al rilascio credenziali. Verifica periodica delle abilitazioni in essere.
Elaboratori	Disponibilità	Guasto nell'elaboratore	3	2	6	Back up automatico su infrastruttura secondaria locale

Telecamere*: tutti i sistemi indicati ai precedenti punti 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12.

4.2.1 Minaccia interna

Componente	Violazione	Evento	D	P	R	Nota e Misure di contenimento
Telecamere	Riservatezza	Uso invasivo del brandeggio (pan & zoom)	3	1	3	Sistema di controllo accessi.
Telecamere	Riservatezza	Uso invasivo delle telecamere mobili	3	2	6	Istruzioni specifiche agli agenti.
Telecamere	Integrità	Manipolazione della configurazione della telecamera per falsarne le immagini	3	1	3	Il sistema di gestione delle telecamere non è manipolabile con accessi diretti esterni alla rete dati degli Enti. Le telecamere non sono manipolabili da remoto.
Telecamere	Disponibilità	Disattivazione volontaria di una telecamera per non riprendere un evento specifico	3	1	3	Richiede specifiche competenze tecniche. Log delle operazioni.
Connessioni	Riservatezza	Cattura immagini pre elaborazione tramite accesso diretto agli apparati di rete	3	1	3	Richiede specifiche competenze tecniche. I sistemi sono protetti da accessi fisici diretti.
Connessioni	Integrità	Manipolazione della configurazione degli apparati di rete per falsare i flussi di immagini	3	1	3	Richiede specifiche competenze tecniche. I sistemi sono protetti da accessi fisici diretti.
Connessioni	Disponibilità	Danneggiamento fisico volontario del cavo o del ponte radio	2	2	4	Posizionamento fisico non facilmente accessibile.
Elaboratori	Riservatezza	Visualizzazione immagini da parte di Amministratori non autorizzabile, tramite pressione su RPD o Agenti	3	2	6	Controllo a campione degli accessi a immagini memorizzate. Log delle operazioni.
Elaboratori	Riservatezza	Utilizzo dei VSS per stalkeraggio	4	2	8	Controllo a campione degli accessi a immagini memorizzate. Log delle operazioni
Elaboratori	Integrità	Interpretazione Volutamente errata delle immagini (es. per evitare sanzione)	3	1	3	Controllo a campione degli accessi a immagini memorizzate. Log delle operazioni
Elaboratori	Disponibilità	Danneggiamento dei server presso PL	3	1	3	I sistemi sono collocati in sala server protetta da accessi fisici.

Telecamere*: tutti i sistemi indicati ai precedenti punti 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12.

4.2.3 Minaccia esterna

Componente	Violazione	Evento	D	P	R	Nota e Misure di contenimento
Telecamere	Riservatezza	Accesso diretto alle telecamere bypassando le protezioni dei sistemi di elaborazione	3	1	3	Cifratura WPA2.
Telecamere	Integrità	Intromissione nelle riprese	3	1	3	Cifratura WPA2.
Telecamere	Disponibilità	Danneggiamento fisico della telecamera	2	2	4	Posizionamento che rende difficoltoso il danneggiamento fisico o il furto della telecamera.
Conessioni	Riservatezza	Intromissione nella comunicazione	3	1	3	Rete dedicata di comunicazione, cifratura WPA2 per i collegamenti wireless o cifratura per i collegamenti su rete fisica VPN.
Conessioni	Integrità	Manipolazione delle riprese	3	1	3	Rete dedicata di comunicazione, cifratura WPA2 per i collegamenti wireless o cifratura per i collegamenti su rete fisica VPN.
Conessioni	Disponibilità	Danneggiamento fisico del cavo o del ponte radio	3	1	3	I cavi e i ponti radio sono di difficile accesso fisico.
Elaboratori	Riservatezza	Aggressione ai sistemi di elaborazione per forzare l'accesso	3	2	6	Richiederebbe una grave compromissione del sistema.
Elaboratori	Integrità	Manipolazione delle immagini per furto delle credenziali	3	1	3	Robustezza e cambio periodico password (ogni 3 mesi).
Elaboratori	Disponibilità	Aggressione con ransomware	3	3	9	Presenti sistemi antivirus e firewall.

Telecamere*: tutti i sistemi indicati ai precedenti punti 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12.

5 Conclusioni

L'analisi del trattamento evidenzia che il trattamento dei dati personali è eseguito in conformità alla normativa vigente, è lecito e necessario ed il Titolare ha adottato misure organizzative e tecniche adeguate alla categoria e tipologia di dati trattati.

La valutazione dei rischi effettuata a partire dai risultati dell'analisi del trattamento non evidenzia rischi "elevati" per i diritti e le libertà degli interessati e le ulteriori misure tecniche ed organizzative in corso di adozione potranno ridurre i rischi residui.

Ai sensi dell'art.36.1 GDPR, il Titolare non ritiene quindi di dover consultare l'Autorità di Controllo prima di procedere al trattamento descritto nel presente documento.