COMUNE DI LABICO

Città Metropolitana di Roma Capitale

COMUNE DI LABICO

(Città Metropolitana di Roma Capitale)

Regolamento per la disciplina dei Sistemi di VIDEOSORVEGLIANZA

Approvato con Delibera di Consiglio Comunale n. 32 del 29/10/2026

Indice

TITOLO I – DISPOSIZIONI GENERALI 3

Art. 1 - Oggetto e normativa di riferimento 3

Art. 2 - Principi generali 5

Art. 3 – Soggetti e definizioni 7

Art. 4 - Valutazione di impatto sulla protezione dei dati 9

Art. 5 - Informativa 10

Art. 6 - Finalità del trattamento mediante sistemi di videosorveglianza 11

TITOLO II - SISTEMI DI VIDEOSORVEGLIANZA 13

Art. 7 - Architettura dei sistemi di videosorveglianza 13

Art. 7-bis – Utilizzo di sistemi di intelligenza artificiale 13

Art. 8 - Modalità di raccolta dei dati 15

Art. 9 - Trattamento e conservazione dei dati 15

Art. 10 - Sicurezza dei dati 17

Art. 11 - Cessazione del trattamento dei dati 19

TITOLO III - ESERCIZIO DEI DIRITTI DEGLI INTERESSATI E ACCESSO ALLE REGISTRAZIONI 19

Art. 12 - Diritti dell'interessato 19

Art. 13 - Accesso alle registrazioni 20

TITOLO IV - DISPOSIZIONI FINALI 21

Art. 14 - Tutela amministrativa e giurisdizionale 21

Art. 15 - Disciplinare-programma 22

Art. 16 - Disciplinari operativi 22

Art. 17 – Allegati 23

Art. 18 - Disposizioni finali e transitorie 23

ALLEGATO Elenco Siti Da Monitorare / Punti Di Installazione Fototrappole 24

Elenco Siti Da Monitorare / Punti Di Installazione Telecamere 24

Elenco Telecamere Lettura Targhe 25

TITOLO I – DISPOSIZIONI GENERALI

Art. 1 - Oggetto e normativa di riferimento

1. Il Regolamento per la disciplina dei sistemi di VIDEOSORVEGLIANZA (da ora anche solo "Regolamento") del Comune di Labico regola le modalità di trattamento dei dati personali mediante sistemi di videosorveglianza e relativi strumenti e applicativi di gestione nell'ambito del territorio di competenza del Comune, stabilendo altresì norme tecniche e organizzative di dettaglio.

2. Il Regolamento concorre a definire la base giuridica, le finalità e le modalità del trattamento, ai sensi dell'articolo 6, paragrafo 3, del Regolamento (UE) 2016/679 e dell'articolo 2-ter del D.lgs. 30 giugno 2003, n. 196, come modificato dal D.L. 8 ottobre 2021, n. 139, convertito con modificazioni dalla Legge 3 dicembre 2021, n. 205.

3. Il presente Regolamento disciplina il trattamento dei dati personali, realizzato mediante sistemi di videosorveglianza attivati nel territorio del Comune nei seguenti ambiti:

- sistema integrato di videosorveglianza per la sicurezza urbana;

- sistema integrato per la lettura delle targhe dei veicoli;

- sistema integrato per l'emergenza mediante colonnine SOS o apparecchiature analoghe;

- sistemi integrati per altri scopi pubblici e/o privati.

4. I suddetti sistemi di videosorveglianza sono da intendersi di tipo "integrato", in quanto consentono la condivisione, integrale o parziale, delle immagini da parte di soggetti diversi attraverso l'utilizzo delle medesime infrastrutture tecnologiche nei termini strettamente funzionali al perseguimento dei rispettivi compiti istituzionali.

4. Il sistema di videosorveglianza finalizzato alla sicurezza pubblica è composto dal complesso di apparecchiature, strumenti, software, dispositivi e ogni altro tipo di tecnologia collegata o comunque connessa ad un centro di controllo, finalizzati alla vigilanza da remoto, ossia a distanza, mediante riprese video. Il sistema può altresì essere integrato, ma non necessariamente connesso, con bodycam, dashcam, telecamere ricollocabili (anche tipo "fototrappola") e Unmanned Aircraft System (sistemi aeromobili a pilotaggio remoto, c.d. "droni", in seguito solo "UAS").

5. Il sistema di videosorveglianza finalizzato ad altri "scopi" (diversi dalla sicurezza pubblica) è composto dal complesso di apparecchiature, strumenti, software, dispositivi e ogni altro tipo di tecnologia collegata o comunque connessa ad un centro di controllo, finalizzati alla vigilanza da remoto, ossia a distanza, mediante riprese video.

6. Le riprese e i fotogrammi, qualora rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi la videosorveglianza rileva sul diritto e le libertà delle persone, in ordine alla propria riservatezza.

7. Con il Regolamento si garantisce che il trattamento dei dati personali, effettuato mediante l'impiego di sistemi di videosorveglianza come sopra definito, gestiti dal Comune di Labico nell'ambito della propria attività istituzionale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza personale. Sono altresì garantiti i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento, avuto riguardo anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico.

8. Il Regolamento per la disciplina dei sistemi di videosorveglianza è adottato nel rispetto dei principi e con riferimento ai seguenti provvedimenti normativi:

a) Regolamento UE 2016/679, del 27 Aprile 2016, "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)";

b) Decreto legislativo 30 Giugno 2003, N. 196 e s.m.i., recante "Codice in materia di protezione dei dati personali";

c) Decreto legislativo 10 Agosto 2018, N. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)";

d) Direttiva UE 2016/680, del 27 Aprile 2016, "relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";

e) Decreto legislativo 18 Maggio 2018, N. 51, recante "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";

f) Legge 3 Dicembre 2021, N. 205, recante "Conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali"; Il D.L. n. 139/2021 è da intendersi come modificato dall'articolo 8-ter del D.L. 10 maggio 2023, n. 51, convertito con modificazioni dalla Legge 3 luglio 2023, n. 87;

g) Linee guida n.3/2019 del 29 gennaio 2020 emesse dal Comitato europeo per la protezione dei dati;

h) Legge del 23 aprile 2009, n. 38, "Conversione in legge, con modificazioni, del decreto-legge 23 febbraio 2009, n. 11, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori";

i) Direttiva del Ministero dell'Interno del 2 marzo 2012 recante "Sistemi di videosorveglianza in ambito comunale";

j) Circolari del Capo della Polizia n. 558/A/421.2/70/456 dell'8 febbraio 2005 e n. 558/A/421.2/70/195960 del 6 agosto 2010;

l) Legge n. 65 del 7 marzo 1986 (Legge quadro sull'ordinamento della Polizia Municipale);

m) Decreto-legge 20 febbraio 2017, n. 14, convertito con modificazioni dalla Legge 18 aprile 2017, n. 48, recante "Disposizioni urgenti in materia di sicurezza delle città";

n) Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, recante il regolamento sul trattamento dei dati effettuato per le finalità di polizia da organi, uffici e comandi di polizia;

o) Provvedimento del Garante per la protezione dei dati personali in materia di videosorveglianza dell'8 aprile 2010 e Provvedimento del 27 novembre 2008 e s.m.i. in materia di amministratori di sistema;

p) Legge 24 novembre 1981, n. 689; D.lgs. 30 aprile 1992, n. 285 (Codice della Strada) e D.lgs. 3 aprile 2006, n. 152, come modificati dal D.L. 8 agosto 2025, n. 116, convertito con modificazioni dalla Legge 3 ottobre 2025, n. 147;

q) Legge 20 maggio 1970, n. 300, con particolare riferimento all'articolo 4;

r) Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (di seguito "Regolamento IA"), come successivamente modificato;

s) Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" (di seguito "Legge IA");

t) Decreto legislativo 7 ottobre 2026, n. 179, recante "Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 [...] in materia di poteri delle Autorità nazionali e di utilizzo dell'intelligenza artificiale nella formazione", pubblicato nella G.U. Serie Generale n. 234 dell'8 ottobre 2026;

u) Linee guida EDPB n. 07/2020 sui concetti di titolare e responsabile del trattamento e Linee guida WP 248 rev.01 in materia di valutazione d'impatto sulla protezione dei dati;

v) Regolamento di Polizia Urbana del Comune di Labico, Patti per l'attuazione della sicurezza urbana sottoscritti con la Prefettura di Roma ai sensi dell'articolo 5 del D.L. n. 14/2017 e atti organizzativi del Comune in materia di protezione dei dati personali.

9. Il Regolamento in particolare, ai sensi dell'articolo 5 del Regolamento UE 2016/679 e articolo 4 della Direttiva (UE) 2016/680 e articolo 3 del D.lgs. n. 51/2018, stabilisce le norme di dettaglio finalizzate all'attuazione, con riguardo ai trattamenti dei dati personali effettuati mediante l'uso di sistemi di videosorveglianza, dei principi, di liceità, correttezza, trasparenza, limitazione delle finalità e minimizzazione dei dati, esattezza, limitazione della conservazione, integrità riservatezza e responsabilizzazione.

10. Possono essere sottoscritti protocolli di intesa, patti per la sicurezza e patti per l'attuazione, convenzioni o accordi, comunque denominati, con soggetti pubblici e soggetti privati, al fine di implementare e condividere sistemi di videosorveglianza per la tutela della sicurezza urbana di cui all'articolo 6 del presente Regolamento.

Art. 2 - Principi generali

1. Il trattamento dei dati personali attraverso il sistema di videosorveglianza avviene secondo i principi generali di:

   a) responsabilizzazione (*accountability*):

      - nel fornire una garanzia di completa accessibilità alle informazioni che riguardano i cittadini in quanto utenti del servizio (*principio di trasparenza*);
      - nella capacità effettiva di rendere conto delle scelte fatte, dei comportamenti, delle azioni attuate e di rispondere alle questioni poste dai portatori di interessi generali (*principio*

della responsività);

- nella capacità effettiva di fare rispettare le norme sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori (*principio della conformità*);

b) protezione dei dati fin dalla progettazione (*privacy by design*) ovvero la necessità di tutelare i dati personali sin dalla fase di sviluppo, progettazione, selezione di un progetto che comporti l'utilizzo di applicazioni, servizi e prodotti per il trattamento di dati personali, creando sistemi che sin dall'inizio dell'attività limitino possibili violazioni dei dati raccolti (articolo 25 comma 1 del GDPR);

c) protezione dei dati per impostazione predefinita (*privacy by default*) ovvero la necessità di implementare misure giuridiche, tecniche e organizzative efficaci e adeguate a garantire che siano trattati solo i dati personali necessari per ciascuna finalità specifica del trattamento, con l'impostazione a priori della massima protezione dei dati attraverso il loro minimo trattamento sia in fase di raccolta sia in fase di trattamento successivo all'acquisizione, secondo i principi di necessità e pertinenza (articolo 25 comma 2 del GDPR).

2. La videosorveglianza è principalmente finalizzata alla tutela della Sicurezza Urbana, come da ultimo formulata dal Decreto legge 20 Febbraio 2017, n. 14, convertito con Legge 18 Aprile 2017, n. 48 come il bene pubblico che afferisce alla vivibilità e al decoro delle città da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio da potenziare con accordi/patti locali ispirati ad una logica di gestione consensuale ed integrata della sicurezza.
3. Si riassumono di seguito i principi per il trattamento dei dati che saranno garantiti nella gestione di sistemi di videosorveglianza comunale:

a) Principio di liceità: il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Esso, infatti, è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui il Comune o il Comando di Polizia Locale sono investiti. La videosorveglianza comunale, pertanto, è consentita senza necessità di consenso da parte degli interessati.

b) Principio di necessità: i sistemi di videosorveglianza sono configurati per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme ed il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.

c) Principio di proporzionalità: nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra una effettiva esigenza di deterrenza. Gli

impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti.

d) Principio di finalità: gli scopi perseguiti devono essere determinati, espliciti e legittimi. È consentita la videosorveglianza come misura complementare volta a tutelare la sicurezza del patrimonio comunale anche nell'ambito di edifici o impianti ove si svolgono attività istituzionali o si garantiscono servizi al cittadino, o comunque con lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.

4. L'uso dei dati personali nell'ambito di cui trattasi, non necessita del consenso degli interessati, in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate alla normativa vigente in materia di protezione dei dati personali.
5. L'angolo di visuale delle riprese su proprietà private e abitazioni è limitato, per quanto tecnicamente possibile, e i fotogrammi potranno essere ulteriormente minimizzati in caso di richiesta degli interessati ovvero in caso di mutamenti della normativa rilevante.
6. Il ricorso a sistemi o funzionalità di intelligenza artificiale nell'ambito dei sistemi di videosorveglianza è informato ai principi di cui all'articolo 3 della Legge 23 settembre 2025, n. 132 e all'articolo 3 del D.lgs. 7 ottobre 2026, n. 179, secondo una prospettiva di garanzia antropocentrica, di uso corretto, trasparente e responsabile dei sistemi e di vigilanza sui rischi per i diritti e le libertà delle persone, ed è disciplinato dall'articolo 7-bis del presente Regolamento.
7. Gli impianti di videosorveglianza non possono essere utilizzati per effettuare controlli sull'attività lavorativa dei dipendenti dell'Ente o di altri datori di lavoro, pubblici o privati, fermo restando quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300 e dall'articolo 18 del presente Regolamento.

Art. 3 – Soggetti e definizioni

1. Dato personale è qualsiasi informazione riguardante una persona fisica identificata o identificabile ("*interessato*"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, i dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
2. L'interessato è la persona fisica a cui si riferiscono i dati personali.
3. Dato anonimo, è il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
4. Trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
5. Impianto di videosorveglianza, è qualunque impianto di ripresa, fissa o mobile, composto da una o più telecamere, in grado di riprendere e registrare immagini e suoni, utilizzato per le finalità

indicate nel presente Regolamento.

6. Sistema di videosorveglianza, è un sistema attraverso il quale si effettua la raccolta, la registrazione, la conservazione ed in generale l'utilizzo di immagini e videoriprese relative a persone fisiche identificate o identificabili, anche indirettamente.
7. Titolare per il trattamento dei dati è il Comune di Labico, Rappresentato legalmente dal Sindaco, a cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali.
8. Altri Designati al trattamento sono le persone fisiche, legate da rapporto di servizio al Comune e preposti dal medesimo al trattamento di dati personali, ai quali il Sindaco stesso demanda alcune responsabilità previste nel presente Regolamento, ai sensi dell'art. 29 del Regolamento (UE) 2016/679, coerentemente all'art. 2-quaterdeciel del D.lgs. n. 196/2003 e, qualora applicabile, all'art. 19 del D.lgs. n. 51/2018. Possono essere designati al trattamento dei dati rilevati con apparecchi di videosorveglianza i soggetti che, per esperienza, capacità ed affidabilità, forniscono le garanzie previste dalle predette norme di cui all'art. 1. Salvo diversa indicazione, designati al trattamento dei dati rilevati con apparecchi di videosorveglianza possono essere:
   a) il Comandante della Polizia locale per le telecamere collegate o comunque connesse alla centrale operativa, nonché le bodycam, dashcam, telecamere ricollocabili (anche tipo "*fototrappola*") e UAS (c.d. droni). Qualora il Responsabile amministrativo dell'Area Organizzativa della Polizia Locale non rivesta la qualifica di ufficiale o agente di polizia giudiziaria, il designato per la videosorveglianza, che richieda la qualifica di cui all'art. 5 della L. n. 65/1986 ovvero di cui all'art. 57 del Codice di Procedura Penale, sarà da individuarsi nell'operatore di grado più elevato.
   b) Altro Responsabile di Area Organizzativa per specifiche finalità perseguite da impianti di videosorveglianza che siano ricomprese nelle attribuzioni e competenze di un Ente Locale e che non prevedano la finalità di sicurezza urbana o prevenzione e accertamento dei reati ovvero la qualifica di polizia stradale.
9. Tali designati vengono puntualmente individuati con apposito atto di nomina del Sindaco, che impartisce direttive e fornisce istruzioni per la gestione ottimale del trattamento di dati mediante videosorveglianza.
10. I designati individuano e nominano, con proprio provvedimento, gli autorizzati alla gestione dell'impianto e al trattamento dei dati nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio e secondo le effettive esigenze operative, determinando profili specifici di autorizzazione al trattamento.
11. Gli autorizzati al trattamento dei dati e alla gestione degli impianti sono le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dai designati al trattamento.
12. L'amministratore o gli amministratori dei sistemi sono figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e alle quali è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione. L'amministratore o gli amministratori dei sistemi sono designati dal titolare del trattamento. In particolare per le telecamere collegate o comunque connesse alla Centrale Operativa, nonché le bodycam, dashcam, le telecamere ricollocabili (anche tipo "fototrappola"), gli UAS, gli amministratori di sistema sono individuati con atto nominativo, previa valutazione dell'esperienza, della capacità e dell'affidabilità, tra gli operatori di Polizia Locale, per gli impianti afferenti alla responsabilità organizzativa dell'Area, ovvero tra il personale del fornitore nominato Responsabile del trattamento, nel rispetto del Provvedimento del Garante

del 27 novembre 2008 e s.m.i.; l'elenco aggiornato degli amministratori di sistema è custodito dal Designato e gli accessi da essi effettuati sono registrati.

13. Con l'atto di nomina ai singoli autorizzati sono affidati i compiti specifici e le puntuali istruzioni e prescrizioni per l'utilizzo dei sistemi di Videosorveglianza.
14. Il Responsabile del trattamento (la cui individuazione, nomina e disciplina è contenuta all'articolo 28 del Regolamento europeo 2016/679 e, laddove applicabile, nell'articolo 18 del Decreto legislativo 18 maggio 2018, n. 51), è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. Qualora, per esigenze connesse alle operazioni di gestione dei dati, o qualsiasi altra attività che comporti l'accesso ai dati per l'esercizio dei sistemi di videosorveglianza, si dovesse rendere necessario ricorrere a Responsabili del Trattamento Esterni all'Amministrazione comunale che svolgono il trattamento per conto del Titolare, questi devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi la conformità alla normativa vigente e garantisca la tutela dei diritti dell'interessato.
15. In ogni caso, la nomina di soggetti esterni all'Amministrazione deve avvenire secondo le vigenti disposizioni organizzative per l'attuazione della normativa in materia di trattamento dei dati personali del Comune di Labico.
16. Il Titolare del trattamento è tenuto a designare il Responsabile della Protezione dei Dati, a normadell'articolo 37 del Regolamento UE 2016/679 e dell'articolo 28 del Decreto legislativo 18 Maggio 2018, n. 51. La nomina del Responsabile della Protezione dei Dati, esterno all'Amministrazione, deve avvenire secondo le vigenti Disposizioni organizzative per l'attuazione della normativa in materia di trattamento dei dati personali del Comune.
17. Per le ulteriori definizioni si rinvia a quanto previsto dall'art. 4 del Regolamento UE 2016/679 e, laddove applicabile, nell'articolo 2 del Decreto legislativo 18 maggio 2018, N. 51.
18. Il Comune può altresì qualificarsi, in virtù di specifici accordi, convenzioni o Patti per l'attuazione della sicurezza urbana, quale Contitolare del trattamento ai sensi dell'articolo 26 del Regolamento (UE) 2016/679 e dell'articolo 17 del D.lgs. n. 51/2018, laddove determini congiuntamente con altri soggetti finalità e mezzi del trattamento. Le Forze di Polizia che accedono agli impianti possono assumere la qualifica di Contitolari ovvero, in ragione della struttura tecnica e organizzativa dell'accesso, di Titolari autonomi. Gli accordi definiscono in modo trasparente ruoli, responsabilità e modalità di esercizio dei diritti degli interessati.
19. Ai fini del presente Regolamento, le nozioni di «sistema di intelligenza artificiale» (sistema di IA), «fornitore», «deployer», «sistema di identificazione biometrica remota», «sistema di riconoscimento delle emozioni» e «sistema di categorizzazione biometrica» sono quelle di cui all'articolo 3 del Regolamento (UE) 2024/1689, richiamate dall'articolo 2 della Legge n. 132/2025 e dall'articolo 1 del D.lgs. n. 179/2026. Il Comune, quando utilizza sotto la propria autorità un sistema di IA nell'ambito dei sistemi di videosorveglianza, assume il ruolo di deployer ai sensi del Regolamento IA.

Art. 4 - Valutazione di impatto sulla protezione dei dati

1. A norma dell'articolo 35, commi 1 e 3, lettera c) del Regolamento (UE) 2016/679, il trattamento di dati mediante sistemi di videosorveglianza, in ragione delle tecnologie impiegate e della predisposizione alla sorveglianza sistematica su larga scala di una zona accessibile al pubblico, è soggetto alla valutazione di impatto sulla protezione dei dati personali da parte del titolare.
2. Laddove ricorrano i presupposti, la valutazione di impatto sulla protezione dei dati personali deve

essere effettuata anche a norma dell'articolo 23 del Decreto legislativo 18 Maggio 2018, n. 51.

3. L'insieme di trattamenti simili svolti mediante sistemi di videosorveglianza può essere esaminato con una singola valutazione. Qualora si ritenga comunque opportuno, può darsi corso a valutazioni separate per ciascun trattamento.
4. La valutazione di impatto sulla protezione dei dati personali è redatta dal designato al trattamento, anche con ausilio di soggetti incaricati quali esperti, dotati di specifiche conoscenze e competenze tecnico-giuridiche, avvalendosi della consulenza del responsabile per la protezione dei dati personali.
5. La valutazione di impatto sulla protezione dei dati personali è adottata secondo le vigenti Disposizioni organizzative per l'attuazione della normativa in materia di trattamento dei dati personali del Comune.
6. La valutazione di impatto è effettuata preventivamente rispetto all'attivazione degli impianti ed è riesaminata prima di ogni implementazione, estensione o modifica significativa degli stessi (quali nuovi siti, nuove funzionalità di analisi video o di lettura targhe, interconnessioni con banche dati, estensione dei tempi di conservazione). Gli impianti eventualmente in esercizio privi di adeguata valutazione di impatto sono sospesi fino al suo completamento.
7. Qualora i sistemi impiegati integrino sistemi di intelligenza artificiale, la valutazione di impatto tiene conto della documentazione e delle istruzioni per l'uso rese dal fornitore ai sensi del Regolamento (UE) 2024/1689 ed è integrata, ove si tratti di sistemi ad alto rischio di cui all'Allegato III del medesimo Regolamento, dalla valutazione d'impatto sui diritti fondamentali di cui all'articolo 27, che può essere condotta congiuntamente alla valutazione di impatto sulla protezione dei dati ai sensi del paragrafo 4 del medesimo articolo.
8. Qualora la valutazione di impatto evidenzi un rischio residuo elevato, il Titolare consulta preventivamente il Garante per la protezione dei dati personali ai sensi dell'articolo 36 del Regolamento (UE) 2016/679 ovvero dell'articolo 24 del D.lgs. n. 51/2018.

Art. 5 - Informativa

1. I soggetti interessati che stanno per accedere o che si trovino in una zona videosorvegliata devono essere informati mediante apposita segnaletica che costituisce Informativa di Primo Livello, o ridotta, nei casi specificamente previsti dalla normativa vigente, con i contenuti minimi previsti dalle vigenti Linee Guida e provvedimenti inerenti dell'Autorità Garante e dell'European Data Protection Board.
2. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, possono essere installati più cartelli, o comunque con modalità tali da rendere possibile a tutti i soggetti che accedono all'area di essere informati della presenza dei dispositivi di videoripresa.
3. Sul sito web istituzionale del Comune e presso gli uffici competenti è resa disponibile l'Informativa di Secondo Livello concernente le finalità del sistema di videosorveglianza, le modalità di raccolta e conservazione dei dati, le modalità di diritto di accesso dell'interessato secondo quanto previsto dal Regolamento UE 2016/679 e dagli articoli 9 e 10 del D.lgs. n. 51/2018.
4. L'informativa di secondo livello è resa direttamente accessibile a partire dall'informativa di primo livello mediante Quick Response Code (QR Code), indirizzo web dedicato o altra modalità idonea a garantire un collegamento diretto e immediato, e dà specifica informazione delle finalità perseguite dai singoli dispositivi o gruppi di dispositivi omogenei, con il relativo posizionamento.
5. Il cartello di primo livello è collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze, ha formato e posizionamento tali da essere chiaramente visibile in ogni

condizione di illuminazione, anche in orario notturno, e indica il periodo di conservazione dei dati; in assenza di tale indicazione si presume che l'impianto consenta la sola visione in tempo reale.

6. Il Comune comunica tempestivamente alla cittadinanza, mediante il sito istituzionale e ulteriori modalità efficaci, l'attivazione degli impianti, i loro incrementi dimensionali e l'eventuale cessazione del trattamento; gli interessati sono informati anche in occasione di eventi e manifestazioni pubbliche.
7. Qualora gli impianti impieghino funzionalità basate su sistemi di intelligenza artificiale, l'informativa di secondo livello ne dà conto in modo chiaro e comprensibile, indicando le funzionalità attive, le finalità, la logica generale di funzionamento e le garanzie di supervisione umana, in attuazione del principio di conoscibilità del funzionamento e di tracciabilità dell'utilizzo di cui all'articolo 14, comma 1, della Legge n. 132/2025, fermi restando, ove applicabili, gli obblighi di trasparenza di cui all'articolo 50 del Regolamento (UE) 2024/1689.

Art. 6 - Finalità del trattamento mediante sistemi di videosorveglianza

1. Le finalità perseguibili dal Comune di Labico mediante l'utilizzo dei sistemi di videosorveglianza sono conformi alle funzioni istituzionali attribuite all'Ente e determinate per:

    a) tutela della "*sicurezza urbana*" e, in via ausiliaria, della sicurezza pubblica ai sensi del D.L. n. 14/2017, in particolare:
        - prevenzione della criminalità, in particolare di tipo predatorio;
        - prevenzione dei fattori di marginalità e di esclusione sociale;
        - protezione e incolumità degli individui;
    b) acquisizione di fonti di prova nell'esercizio delle funzioni di polizia giudiziaria ai sensi D.P.R. n. 447/1988, L. n. 65/1986, D.lgs. n. 51/2018;
    c) prevenzione, accertamento e repressione, ove consentito, degli illeciti amministrativi, anche ai sensi della L. n. 689/1981;
    d) tutela degli immobili di proprietà o in uso all'Amministrazione, delle infrastrutture e dei beni pubblici ai sensi del R.D. n. 262/1942 e R.D. 1398/1930;
    e) tutela ambientale, attraverso il monitoraggio, il contrasto e la repressione del fenomeno dell'abbandono illecito di rifiuti ai sensi del D.lgs. 152/2006 e, per quanto applicabile, del D.P.R. 15/2018;
    f) supporto nel monitoraggio del traffico e dei parcheggi, nonché nella rilevazione e nella contestazione delle infrazioni ai sensi dell'art. 11 del D.lgs. n. 285/1992, c.d. Codice della Strada, nel rispetto delle norme che regolano la materia e disciplinano le categorie di dispositivi di videosorveglianza consentiti, nonché le modalità di rilevazione e contestazione;
    g) attuazione delle ordinanze contingibili e urgenti adottate dal Sindaco, ai sensi degli artt. 50 e 54 del T.U.E.L.

2. Il Titolare del Trattamento promuove ed attua, nell'ambito delle competenze istituzionali attribuite in materia di sicurezza urbana e di sicurezza integrata e in relazione alla prevenzione della criminalità in ambito predatorio, attività ed interventi di controllo del territorio unitamente alle Forze di Polizia preposte alla tutela della sicurezza e dell'ordine pubblico, nel rispetto delle previsioni di cui al D. Lgs. n. 51 del 18 maggio 2018. In tale contesto, il Corpo di Polizia Locale costituisce l'articolazione fondamentale dell'Ente a cui afferiscono gli impianti di videosorveglianza e sistemi di sicurezza tecnologica finalizzati al controllo

delle aree e delle attività soggette a rischio. L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre forze di polizia a competenza generale, deve essere specificatamente disciplinato con appositi patti o convenzioni.

3. Gli impianti di videosorveglianza non possono essere utilizzati, in base alla vigente normativa, sulla tutela dei diritti dei lavoratori per effettuare controlli sull'attività lavorativa dei dipendenti. Se dagli impianti derivi la possibilità di controllo a distanza dei lavoratori devono espletarsi gli adempimenti previsti dall'art. 4 della L. 300/1970, procedendo ad una dovuta informativa alle rappresentanze sindacali ovvero, ove non si raggiunga un accordo verbalizzato, tracciando il riscontro negativo delle rappresentanze sindacali, all'acquisizione dell'autorizzazione dell'Ispettorato del Lavoro.

4. Il Titolare del Trattamento, nel rispetto della normativa vigente, non installa o utilizza impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici di cui all'art. 4, n. 14), del G.D.P.R. in luoghi pubblici o aperti al pubblico ("*larga scala*"), ed è vietato l'utilizzo dei suddetti sistemi qualora associati agli impianti di videosorveglianza fino all'eventuale entrata in vigore di una disciplina legislativa della materia che lo consenta nell'ambito dell'ordinamento della polizia municipale.

5. Le specifiche finalità perseguite dai singoli impianti di videosorveglianza installati devono essere valutate in apposite Valutazioni di Impatto sulla Protezione dei dati personali ai sensi dell'art. 35 G.D.P.R. e, ove applicabile, dell'art. 23 D.lgs. n. 51/2018. Delle finalità effettivamente perseguite deve essere effettuato un giudizio di compatibilità e di ragionevole aspettativa dell'interessato nell'ambito dei singoli impianti. Ogni impianto che persegua finalità distinte deve essere appositamente notiziato e soggetto alle misure di trasparenza verso gli interessati applicabili ai sensi degli artt. 13 e 14 del G.D.P.R. o, laddove applicabili, ai sensi degli artt. 10 e ss. del D.lgs. n. 51/2018, nonché ai sensi dell'art. 12 del presente Regolamento.

6. Gli impianti di videosorveglianza installati per finalità di sicurezza urbana non possono essere impiegati per finalità differenti, ivi compreso l'accertamento di violazioni amministrative a norma dell'articolo 13 della Legge 24 novembre 1981, n. 689, salvo che il Titolare comprovi, per lo specifico trattamento ulteriore, la sussistenza di un'autonoma base giuridica e la compatibilità con la finalità originaria, dandone conto nella valutazione di impatto e nell'informativa. Sono fatte salve le finalità di accertamento previste da specifiche disposizioni di legge, tra cui quelle introdotte dal D.L. 8 agosto 2025, n. 116, convertito con modificazioni dalla Legge 3 ottobre 2025, n. 147, che ha novellato l'articolo 255 del D.lgs. 3 aprile 2006, n. 152 e l'articolo 201 del D.lgs. 30 aprile 1992, n. 285, nonché l'impiego dei dispositivi di rilevamento delle violazioni al Codice della Strada debitamente approvati od omologati.

7. Qualora il Comune di Labico, attraverso la Polizia Locale, per compiti, attribuzioni e finalità proprie, acceda agli impianti di terzi, siano essi privati o soggetti pubblici, acquisisce la qualifica di Titolare del Trattamento del dato personale, salvo che tale accesso non avvenga nell'ambito di apposite convenzioni o accordi istituzionali o partenariati pubblico-privati che individuino un differente ruolo ai sensi degli artt. 4, 26 o 28 del Reg. (UE) 2016/679 ovvero del D.lgs. n. 51/2018, qualora applicabile.

TITOLO II - SISTEMI DI VIDEOSORVEGLIANZA

Art. 7 - Architettura dei sistemi di videosorveglianza

1. I sistemi di videosorveglianza prevedono il trattamento di dati personali che possono essere rilevati da telecamere, anche munite di algoritmi di analisi video, di metadatazione, di conteggio delle persone e verifica dei comportamenti (nei limiti e alle condizioni di cui all'articolo 7-bis), o dispositivi di "lettura targhe" interfacciati con "black-list" o altre banche dati.
2. Il sistema di videosorveglianza, in relazione alle esigenze della Polizia locale, può essere integrato, ma non necessariamente connesso, con bodycam, dashcam, UAS, telecamere ricollocabili (anche tipo "*foto-trappola*"), altri dispositivi mobili (anche con generazione di allarmi da remoto per il monitoraggio attivo). L'effettivo impiego di tali dispositivi sarà stabilito nel disciplinare-programma di cui all'articolo 15 del presente Regolamento. Le modalità e istruzioni di impiego saranno fornite nel disciplinare operativo di cui all'articolo 16 del presente Regolamento.
3. Il personale addetto riceverà apposito disciplinare tecnico sull'utilizzo delle bodycam, delle dashcam e degli UAS, nonché l'informativa sul trattamento dei loro dati personali che indirettamente potrebbero essere trattati in relazione all'evolversi degli scenari che fanno insorgere situazioni di pericolo, turbamento dell'ordine e della sicurezza pubblica e nel caso di pericolo imminente per persone e/o cose o di insorgenza di situazioni di criticità.
4. Nel rispetto delle finalità previste nel presente Regolamento, dalle immagini di videosorveglianza potranno anche essere acquisiti elementi utili all'accertamento di violazioni amministrative, nei limiti di cui all'articolo 6 del presente, nel rispetto delle vigenti normative e regolamenti.

Art. 7-bis – Utilizzo di sistemi di intelligenza artificiale

1. Le disposizioni del presente articolo si applicano ai componenti hardware e software dei sistemi di videosorveglianza, inclusi i software di gestione, di analisi video e di lettura targhe, che integrano sistemi di intelligenza artificiale come definiti dall'articolo 3, punto 1), del Regolamento (UE) 2024/1689. Rispetto a tali sistemi il Comune può operare quale "*deployer*" ed è tenuto agli obblighi previsti dal Regolamento IA, dalla Legge n. 132/2025 e dal D.lgs. n. 179/2026, in aggiunta a quelli derivanti dalla normativa in materia di protezione dei dati personali.
2. L'utilizzo dei sistemi di intelligenza artificiale avviene in funzione esclusivamente strumentale e di supporto all'attività degli operatori, nel rispetto dell'autonomia e del potere decisionale della persona, che resta l'unica responsabile dei provvedimenti e degli atti adottati, ai sensi dell'articolo 14, comma 2, della Legge n. 132/2025. Nessun atto di accertamento o di contestazione, nessuna segnalazione all'Autorità giudiziaria e nessun altro provvedimento che produca effetti giuridici nei confronti dell'interessato può essere adottato unicamente sulla base dell'esito prodotto da un sistema di IA (quale un allarme o una corrispondenza con una "black-list"), senza la verifica di un operatore autorizzato, nel rispetto dell'articolo 22 del Regolamento (UE) 2016/679 e dell'articolo 8 del D.lgs. n. 51/2018.
3. È in ogni caso escluso l'impiego delle pratiche di intelligenza artificiale vietate dall'articolo 5 del Regolamento (UE) 2024/1689. Il Comune, inoltre, non installa né utilizza, mediante gli impianti di

videosorveglianza: a) sistemi di identificazione biometrica remota, in tempo reale o a posteriori, ivi compresi i sistemi di riconoscimento facciale; b) sistemi di riconoscimento delle emozioni; c) sistemi di categorizzazione biometrica; d) sistemi di valutazione del rischio che una persona commetta un reato basati sulla profilazione o sulla valutazione dei tratti della personalità; ciò fino all'eventuale entrata in vigore di una disciplina legislativa che ne consenta l'utilizzo e ne stabilisca le garanzie.

4. Prima dell'acquisizione, dell'attivazione o dell'aggiornamento di un sistema o di una funzionalità basata su intelligenza artificiale, il Designato competente, con il supporto del Responsabile della Protezione dei Dati e dell'Amministratore di sistema: a) acquisisce dal fornitore documentazione idonea a comprovare se il componente costituisca un sistema di IA, la relativa classificazione del rischio ai sensi del Regolamento IA, le istruzioni per l'uso, la dichiarazione di conformità UE e, ove prevista, la registrazione nella banca dati dell'Unione; b) verifica che i contratti di fornitura e gli atti di nomina a Responsabile del trattamento ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 disciplinino l'eventuale utilizzo dei dati per l'addestramento dei modelli, escluso salvo specifica e motivata autorizzazione del Titolare, la localizzazione dei dati e la cooperazione negli adempimenti previsti dal Regolamento IA; c) promuove l'aggiornamento della valutazione di impatto di cui all'articolo 4; d) iscrive il sistema in un apposito inventario dei sistemi di IA in uso presso l'Ente. Le funzionalità basate su intelligenza artificiale sono disattivate per impostazione predefinita e sono abilitate solo all'esito di tali adempimenti.

5. Qualora il sistema sia classificato ad alto rischio, il Comune, quale "*deployer*", adotta le misure previste dall'articolo 26 del Regolamento (UE) 2024/1689 e, in particolare: utilizza il sistema conformemente alle istruzioni per l'uso; affida la sorveglianza umana a persone fisiche dotate della competenza, della formazione e dell'autorità necessarie; verifica la pertinenza dei dati di input sotto il proprio controllo; monitora il funzionamento del sistema; conserva i log generati automaticamente per un periodo adeguato alla finalità e comunque non inferiore a sei mesi, salvo diversa disposizione del diritto dell'Unione o nazionale, in particolare in materia di protezione dei dati personali; sospende l'uso del sistema e informa senza ritardo il fornitore e l'autorità di vigilanza del mercato in caso di rischio o di incidente grave.

6. Ai fini del presente articolo, l'Agenzia per la cybersicurezza nazionale è autorità di vigilanza del mercato e punto di contatto unico ai sensi degli articoli 5 e 6 del D.lgs. n. 179/2026, mentre il Garante per la protezione dei dati personali è autorità di vigilanza del mercato limitatamente a quanto previsto dall'articolo 74, paragrafo 8, del Regolamento IA, che ricomprende i sistemi ad alto rischio utilizzati a fini di attività di contrasto. Restano ferme le competenze del Garante in materia di protezione dei dati personali.

7. Il personale che utilizza o supervisiona i sistemi di intelligenza artificiale riceve una formazione adeguata e periodicamente aggiornata, ai sensi dell'articolo 4 del Regolamento (UE) 2024/1689, dell'articolo 14, comma 3, della Legge n. 132/2025 e delle linee guida adottate ai sensi dell'articolo 40 del D.lgs. n. 179/2026, comprensiva dei limiti dei sistemi, del rischio di errori e distorsioni dei risultati, della tendenza a fare eccessivo affidamento sugli output e delle modalità di esercizio della sorveglianza umana.

8. I sistemi di intelligenza artificiale non possono essere impiegati per il monitoraggio o la valutazione del personale dell'Ente; resta fermo quanto previsto dall'articolo 4 della Legge n. 300/1970, dall'articolo 11 della Legge n. 132/2025 e dagli articoli 41 e 42 del D.lgs. n. 179/2026.

9. Le disposizioni del presente articolo si applicano fatta salva la disciplina speciale per l'utilizzo di sistemi di intelligenza artificiale per l'attività di polizia di cui all'articolo 24, comma 2, lettera h), della Legge n. 132/2025, nonché in caso di modifiche del Regolamento (UE) 2024/1689 e delle relative date di applicazione.

Art. 8 - Modalità di raccolta dei dati

1. I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da sistemi di dispositivi di videosorveglianza che inquadrano luoghi pubblici e aperti al pubblico, nonché in immobili di proprietà o in uso al Comune di Labico, ubicati nel territorio comunale.
2. I dispositivi di cui al precedente comma, finalizzati alla tutela della sicurezza urbana, consentono riprese video anche con utilizzo di algoritmi di analisi, nei limiti di cui all'articolo 7-bis, possono essere dotate di brandeggio e di zoom ottico e sono collegate alla centrale operativa del Comando di Polizia locale, che potrà, esclusivamente per il perseguimento dei fini istituzionali, digitalizzare o indicizzare le immagini.
3. L'utilizzo del "*brandeggio*" (movimento di rotazione di bracci mobili di strumenti o apparecchiature) e dello zoom da parte del Designato e degli autorizzati al trattamento deve essere conforme alle finalità dell'impianto riportate all'articolo 6 del presente Regolamento.
4. Le immagini videoregistrate sono conservate per il periodo indicato nell'articolo 9. Decorso il termine di conservazione il sistema di videoregistrazione provvede in automatico alla loro cancellazione, ove tecnicamente possibile, mediante sovra-registrazione, con modalità tali da rendere non più utilizzabili i dati cancellati.

Art. 9 - Trattamento e conservazione dei dati

1. I dati personali oggetto di trattamento effettuato mediante sistemi di videosorveglianza di cui al presente Regolamento, nel rispetto delle misure minime indicate dalla normativa relative alla protezione delle persone fisiche, sono:
    a) trattati in modo lecito, secondo correttezza e trasparente;
    b) raccolti e registrati per le finalità di cui al precedente articolo 6 e resi utilizzabili per operazioni compatibili con esse;
    c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati, esatti e, se necessario, aggiornati;
    d) conservati, per quanto riguarda i dati raccolti mediante le telecamere collegate alla centrale operativa, per un periodo ordinariamente non superiore a sette (7) giorni successivi alla rilevazione, ai sensi dell'articolo 6, comma 8, del D.L. 23 febbraio 2009, n. 11, convertito dalla Legge 23 aprile 2009, n. 38, che può essere esteso tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati. Termini specifici di conservazione dei dati in relazione alle singole finalità sono eventualmente individuati dalla legge ovvero dal disciplinare-programma e specificamente esaminati nella valutazione di impatto sulla protezione dei dati di cui all'articolo 4;

e) conservati, per le telecamere a tutela del solo patrimonio comunale o non rientranti nelle finalità e patti per l'attuazione della Sicurezza Urbana (o per altre telecamere non collegate alla centrale operativa della Polizia Locale o comunque non gestite da operatori di Polizia locale), per un periodo non superiore a quarantotto (48) ore successive alla rilevazione, fatte salve speciali esigenze di sicurezza urbana e sicurezza pubblica o di gestione integrata.

2. La disponibilità di immagini costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'attività della Polizia Locale e delle altre Forze dell'Ordine sul territorio comunale, secondo le indicazioni del Comitato provinciale per l'ordine e la sicurezza pubblica e in applicazione di accordi o patti locali per l'attuazione della sicurezza urbana. Le immagini possono altresì essere utilizzate da parte della Polizia Giudiziaria per indagini di iniziativa o delegate. Le telecamere dei suddetti impianti consentono, tecnicamente, riprese video a colori o in bianco/nero a seconda della tecnologia del relativo impianto, anche con utilizzo di appositi software; possono essere dotate di brandeggio e di zoom ottico e sono collegate alla centrale operativa del Comando di Polizia Locale e, qualora regolamentato con appositi accordi e ricompreso nell'ambito dei Patti per l'Attuazione della Sicurezza Urbana, alle Sale operative delle Forze dell'Ordine ad esse connesse per il perseguimento dei fini istituzionali.

3. Il trattamento dei dati personali mediante sistemi integrati per l'emergenza, come le colonnine SOS o apparecchiature analoghe, è effettuato a tutela delle persone che transitano o si trovano nell'area interessata ove ubicato l'impianto, in applicazione di accordi o patti locali per l'attuazione della sicurezza urbana.

4. L'utilizzo di impianti elettronici di rilevamento automatico delle violazioni delle disposizioni in materia di circolazione stradale costituisce trattamento dei dati personali, analogamente al trattamento derivante da sistemi di videosorveglianza, ed è sottoposto ai requisiti di omologazione ovvero alle modalità di accertamento disciplinate dal Codice della Strada.

5. Gli operatori di Polizia Locale, nello svolgimento di servizi operativi e di controllo del territorio, possono essere dotati di *Body Cam* (ossia sistemi di ripresa indossabili) e di *Dash Cam* (telecamere a bordo veicoli di servizio) in conformità alle indicazioni dettate dal Garante per la protezione dei dati personali con nota 26 luglio 2016, prot. n. 49612, contenente le prescrizioni generali di utilizzo dei predetti dispositivi e, per i trattamenti effettuati per finalità di polizia, nel rispetto del D.P.R. 15 gennaio 2018, n. 15, previa valutazione di impatto. L'impiego di Body Cam, Dash Cam o Droni è sottoposto a Valutazione di Impatto sulla Protezione dei Dati Personali e alla Consultazione Preventiva del Garante, ai sensi dell'art. 36 del Reg. (UE) 2016/679 e dell'art. 24 del D.lgs. n. 51/2018, salvo modifiche degli orientamenti espressi e modifiche alla normativa rilevante in tema.

6. Il Comando di Polizia Locale può dotarsi inoltre di telecamere riposizionabili, anche del tipo "*foto-trappola*", con generazione di allarmi da remoto per il monitoraggio attivo, nonché di apparati di videosorveglianza modulare riposizionabili, da installare secondo necessità, qualora gli eventuali illeciti riscontrabili sul territorio non siano altrimenti accertabili con le ordinarie metodologie di indagine.

7. Il Comando di Polizia Locale può altresì dotarsi di ogni altra tecnologia di ripresa video e di captazione di immagini come i Sistemi Aeromobili a Pilotaggio Remoto – droni – in conformità alla normativa vigente e in particolare alla regolamentazione adottata dall'Ente Nazionale per l'Aviazione Civile e al Codice della Navigazione.

8. Ulteriori prescrizioni sull'utilizzo dei dispositivi indicati ai commi 5, 6 e 7 del presente articolo saranno impartite dal Comandante del Corpo di Polizia Locale.

9. Le immagini videoregistrate dalle telecamere sono conservate per un periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione qualora rientrino nell'ambito di applicazione di cui all'art. 6 comma 8 del D-L. n. 11/2009, e possono essere estesi tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati, anche in riferimento ai varchi lettura targhe che perseguano tale finalità, e previa segmentazione degli accessi da effettuare in relazione a specifiche ed evidenti esigenze investigative e di Polizia Giudiziaria, nonché specifiche richieste da parte dell'Autorità giudiziaria.

10. I dati acquisiti nell'ambito dei rilievi degli incidenti stradali potranno essere conservati per periodi di tempo maggiore per attività di analisi, studio, divulgazione e prevenzione, a patto che i soggetti ripresi non siano riconoscibili e siano rispettati i principi di essenzialità del dato conservato.

11. I dispositivi di fototrappolaggio di cui al comma 6 sono impiegati esclusivamente nei siti individuati con apposito atto di indirizzo o nel Disciplinare-Programma ovvero negli areali indicati in apposito elenco pubblicamente accessibile, per finalità di prevenzione e accertamento degli illeciti in materia di abbandono di rifiuti, previa collocazione dell'informativa di primo livello, salvo che l'impiego avvenga per finalità di polizia giudiziaria nel rispetto del D.lgs. n. 51/2018. I dispositivi non possono essere distolti dalle finalità che sono loro proprie.

12. I dispositivi di fototrappolaggio devono: a) essere dotati di marcatura CE estesa all'intero prodotto; b) trasmettere le immagini, mediante canali cifrati conformi ai protocolli di trasmissione sicura più recenti, esclusivamente al sistema di gestione e ai dispositivi autorizzati; c) prediligere forme di conservazione remota o cloud; qualora la conservazione avvenga su memorie locali devono essere in ogni caso cifrate e svuotate secondo i tempi di cui al presente articolo; d) generare notifiche in caso di manomissione; e) essere orientati in modo da limitare la ripresa all'area oggetto di monitoraggio, escludendo per quanto possibile proprietà private e aree non pertinenti.

13. Le immagini e i dati rilevati dai varchi di lettura targhe sono trattati esclusivamente per le finalità per le quali i varchi sono stati attivati. L'interconnessione con banche dati esterne (quali elenchi di veicoli rubati o privi di copertura assicurativa) è ammessa solo ove prevista da una norma di legge o da accordi con le Autorità competenti, ed è descritta nella valutazione di impatto.

Art. 10 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati presso la centrale di registrazione, alla quale può accedere il solo personale autorizzato secondo istruzioni che devono essere impartite dal designato al trattamento dei dati, secondo quanto previsto dall'art. 29 del Regolamento UE 2016/679 e dall'art. 2-quaterdecies del Decreto legislativo 196/2003 e ss.mm.

2. In particolare, la centrale di registrazione delle telecamere del sistema di videosorveglianza finalizzato alla sicurezza cittadina, collegate o comunque connesse alla centrale operativa della Polizia locale, è ubicata presso la sede della Polizia locale, in specifico locale tecnico, il cui accesso è riservato al personale abilitato. I flussi video delle telecamere di campo sono trasmessi in via prioritaria mediante rete in fibra

ottica dedicata; residualmente in modalità wireless, in modalità crittografata. I dati raccolti sono inviati a server destinati esclusivamente alla videosorveglianza. Mediante quest'ultimi, le immagini sono rinviate alle postazioni di controllo. I flussi video sono registrati su Network Attached Storage dedicato unicamente alla videosorveglianza. L'infrastruttura logica di rete locale non è in condivisione con altre infrastrutture di rete.

3. In particolare, l'accesso agli ambienti in cui è ubicata una postazione di controllo è consentito solamente al personale autorizzato e per scopi connessi alle finalità previste nonché alle società incaricate alla manutenzione degli impianti debitamente nominate Responsabili del trattamento, alla pulizia dei locali e per occasionali motivi istituzionali. L'accesso è comunque soggetto ad autorizzazione da parte del titolare o del designato al trattamento.
4. L'accesso alle centrali di registrazione e alle postazioni di controllo è regolato dal disciplinare-programma di cui all'articolo 15 e dai disciplinari operativi di cui all'articolo 16.
5. Il designato impartisce idonee istruzioni atte ad evitare assunzioni o rilevamenti abusivi di dati, da parte dei soggetti terzi che accedono ai locali.
6. Il designato individua e nomina gli autorizzati in numero sufficiente a garantire l'efficace ed efficiente gestione del servizio di videosorveglianza.
7. Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.
8. In ogni caso, prima dell'utilizzo degli impianti, essi sono istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento, del presente Regolamento e degli ulteriori provvedimenti adottati.
9. Gli autorizzati al trattamento sono dotati di proprie credenziali di autenticazione al sistema.
10. Il sistema deve essere fornito di dati di "*log*" relative all'accesso e alle operazioni eseguite da ciascun utente, le cui informazioni dovranno essere conservate per la durata di almeno sei mesi.
11. L'accesso da remoto ai dati rilevati con i sistemi di videosorveglianza è consentito esclusivamente al personale autorizzato e al Designato, mediante canali di trasmissione sicuri (quali Virtual Private Network), autenticazione forte e dispositivi inventariati e protetti con idonee misure di sicurezza informatica.
12. I monitor delle postazioni di controllo sono collocati in modo da non consentire la visione delle immagini, neanche occasionale, a persone non autorizzate e sono dotati di blocco automatico con autenticazione all'accesso.
13. L'impianto prevede la cifratura dei flussi video, idonee misure di backup e la segregazione della rete rispetto ad altri flussi informativi dell'Ente; gli apparati di ripresa connessi a reti informatiche sono protetti contro i rischi di accesso abusivo di cui all'articolo 615-ter del Codice penale.
14. I log di accesso degli amministratori di sistema sono conservati per almeno sei mesi e comunque non oltre un anno, salvo motivate esigenze di sicurezza informatica; per i trattamenti eventualmente rientranti nell'ambito del D.P.R. n. 15/2018 i log rispettano i requisiti di cui all'articolo 24 del medesimo decreto.

15. I supporti removibili contenenti copie di immagini sono custoditi in armadi dotati di serratura fino alla consegna alle autorità competenti o alla distruzione; della distruzione dei supporti e dei dispositivi di archiviazione, anche se affidata a soggetti esterni, è redatto verbale o acquisita documentazione comprovante la tecnica utilizzata.

Art. 11 - Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti, ceduti o conservati secondo quanto previsto dal Regolamento (UE) 2016/679 e, ove applicabile, dal Decreto legislativo 18 maggio 2018, n. 51. In particolare, i dati possono essere: a) distrutti, mediante tecniche che garantiscano l'impossibilità di ricostruzione del supporto; b) cancellati mediante sovrascrittura sicura o smagnetizzazione del supporto; c) ceduti ad altro titolare solo per trattamenti compatibili con gli scopi della raccolta e in presenza di idonea base giuridica; d) conservati per fini esclusivamente istituzionali, nei termini di legge applicabili. Delle operazioni è redatto apposito verbale; ove esse siano eseguite da un soggetto esterno nominato Responsabile del trattamento, è acquisita prova documentale delle tecniche utilizzate.

TITOLO III - ESERCIZIO DEI DIRITTI DEGLI INTERESSATI E ACCESSO ALLE REGISTRAZIONI

Art. 12 - Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, a seguito di presentazione di apposita istanza, può esercitare i diritti di cui agli articoli da 15 a 22 e 34 del Regolamento (UE) 2016/679 e, per i trattamenti rientranti nell'ambito di applicazione del D.lgs. 18 maggio 2018, n. 51, i diritti di cui agli articoli da 9 a 14 del medesimo decreto, con le limitazioni ivi previste. In particolare, l'interessato ha diritto:

    a) di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati e alle informazioni di cui all'articolo 15 del Regolamento (UE) 2016/679, nonché copia dei dati, previo oscuramento dei dati riferibili a terzi;

    b) di ottenere la cancellazione dei dati (articolo 17) e la limitazione del trattamento (articolo 18), ivi compresa la conservazione delle immagini oltre il termine ordinario quando necessarie per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

    c) di opporsi al trattamento per motivi connessi alla propria situazione particolare (articolo 21);

    d) di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (articolo 22) e di ricevere, qualora il trattamento coinvolga sistemi di intelligenza artificiale, informazioni sul loro funzionamento ai sensi dell'articolo 14 della Legge n. 132/2025 e, ove applicabile, la spiegazione di cui all'articolo 86 del Regolamento (UE) 2024/1689;

    e) di essere informato senza ingiustificato ritardo della violazione dei dati personali che lo riguardano, quando suscettibile di presentare un rischio elevato per i suoi diritti e libertà (articolo 34).

2. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

3. Le istanze sono presentate al Titolare o al designato al trattamento. Nell'esercizio dei diritti di cui al comma 1, l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi.
4. Nel caso in cui le istanze non siano adeguatamente riscontrate, l'interessato ha la facoltà di proporre reclamo al Garante per la protezione dei dati personali ai sensi dell'articolo 77 del Regolamento (UE) 2016/679 e delle corrispondenti disposizioni del D.lgs. n. 51/2018, fatte salve le ulteriori forme di tutela amministrativa e giurisdizionale.
5. Le istanze sono riscontrate entro un mese dal ricevimento; tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste, dandone comunicazione all'interessato entro il primo mese. Il riscontro è gratuito, salvo il caso di richieste manifestamente infondate o eccessive, di cui il Titolare dimostra il carattere.
6. In considerazione della natura intrinseca delle immagini registrate, raccolte in tempo reale e riferite a un fatto obiettivo, non è in concreto esercitabile il diritto di rettifica; resta fermo il diritto di ottenere la cancellazione o la limitazione dei dati trattati in violazione di legge.
7. Per i trattamenti rientranti nell'ambito del D.lgs. n. 51/2018, l'esercizio dei diritti può essere ritardato, limitato o escluso nei casi previsti dall'articolo 14 del medesimo decreto; durante il procedimento penale o dopo la sua definizione, la rettifica, la cancellazione o la limitazione dei dati possono essere richieste con le modalità di cui all'articolo 116 del Codice di procedura penale.

Art. 13 - Accesso alle registrazioni

1. Al di fuori dei diritti dell'interessato, l'accesso alle registrazioni della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente e nel rispetto di quanto disciplinato dal presente regolamento.
2. Ogni richiesta deve essere specifica, formulata per iscritto, motivata e indirizzata al designato del trattamento dei dati tempestivamente e comunque entro il termine di conservazione delle immagini di cui all'articolo 9.
3. L'accesso ai documenti amministrativi di cui alla Legge 7 agosto 1990, n. 241 avente ad oggetto le immagini è consentito nei soli limiti in cui il richiedente dimostri un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente tutelata, previo oscuramento o minimizzazione dei dati riferibili a terzi e fermi i limiti derivanti dal segreto investigativo. È fatto salvo, nel rispetto delle vigenti normative speciali, il diritto di accesso ai documenti amministrativi derivanti dalla visione delle immagini da parte degli organi di polizia.
4. Per finalità di indagine, l'Autorità giudiziaria e la polizia giudiziaria possono richiedere e acquisire copia delle registrazioni in formato digitale, formulando specifica richiesta scritta, qualora non abbiano accesso diretto alle immagini.
5. Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, copia delle riprese in formato digitale può essere richiesta e acquisita dall'organo di polizia stradale che ha proceduto ai rilievi e in capo al quale è l'istruttoria relativa all'incidente.

6. Salvo il caso si tratti di documenti già acquisiti dall'Autorità giudiziaria, nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'art. 391-quater c.p.p., può richiedere e acquisire copia delle riprese in formato digitale.
7. Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al designato del trattamento, anche ai sensi dell'articolo 18, paragrafo 1, lettera c), del Regolamento (UE) 2016/679, che i filmati siano conservati oltre i termini di cui all'articolo 9, per essere messi a disposizione dell'organo di polizia procedente. La richiesta deve obbligatoriamente pervenire entro i termini di conservazione previsti, onde evitare la cancellazione delle immagini. Spetta all'organo di polizia procedente presentare richiesta di acquisizione dei filmati. Tale richiesta deve pervenire entro 30 giorni dalla data dell'evento, decorsi i quali i dati non saranno ulteriormente conservati.
8. In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'autorizzato dal designato del trattamento dei dati deve annotare le operazioni eseguite al fine di acquisire i filmati per riversarli su supporto digitale, con lo scopo di garantire la genuinità dei dati stessi.
9. Possono comunque essere divulgate, in casi eccezionali, immagini provenienti dagli impianti di videosorveglianza, previa anonimizzazione di ogni dato che consenta l'identificazione dei soggetti.
10. La consegna della copia delle riprese in formato digitale prevede il pagamento delle relative spese, individuate con apposita deliberazione di Giunta comunale riguardante le tariffe di accesso ai documenti amministrativi.
11. Le richieste di accesso alle immagini presentate da soggetti esterni all'Ente e accolte sono annotate in un apposito Registro degli accessi, nel quale sono riportati la data e l'ora dell'accesso, l'identificazione del richiedente, i dati oggetto di accesso, gli estremi e la motivazione dell'autorizzazione, le eventuali osservazioni e la sottoscrizione del richiedente.
12. Le immagini sono consegnate secondo la procedura stabilita dal Designato, previa verifica di minimizzazione dei dati personali riferibili a terzi; la consegna può essere effettuata direttamente all'Autorità giudiziaria destinataria, previa richiesta formale e secondo le previsioni del Codice di procedura penale.

TITOLO IV - DISPOSIZIONI FINALI

Art. 14 - Tutela amministrativa e giurisdizionale

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dall'articolo 77 e seguenti del Regolamento (UE) 2016/679 e dall'articolo 37 e seguenti del Decreto legislativo 18 Maggio 2018, n. 51.
2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti dell'articolo 4 e seguenti della Legge 7 Agosto 1990, N. 241, è il Designato al trattamento dei dati personali, così come individuato dal precedente articolo 3.
3. La mancata osservanza degli obblighi previsti dal presente Regolamento comporta l'applicazione di sanzioni disciplinari, coerentemente con il vigente Codice di comportamento, e, nei casi previsti dalla

legge, di sanzioni amministrative o penali. Restano ferme le sanzioni previste dal D.lgs. n. 179/2026 per le violazioni del Regolamento (UE) 2024/1689.

Art. 15 - Disciplinare-programma

1. La Giunta comunale, sulla base degli indirizzi e principi contenuti nel presente Regolamento, con propria deliberazione, adotta, su proposta del Designato al trattamento dei dati personali il "disciplinare-programma per l'utilizzo degli impianti di videosorveglianza".
2. Il disciplinare-programma può individuare anche qualsiasi altro dettaglio, specificazione, regolamentazione della videosorveglianza nel rispetto del presente Regolamento.
3. Il disciplinare-programma individua in particolare: l'elenco aggiornato degli impianti e dei siti con le relative finalità; i tempi di conservazione per ciascuna categoria di impianto; le funzionalità di analisi video e i sistemi di intelligenza artificiale abilitati, con la relativa classificazione del rischio; le interconnessioni con altre banche dati; le modalità di accesso delle Forze di Polizia in attuazione dei patti e degli accordi sottoscritti.

Art. 16 - Disciplinari operativi

1. Il Designato al trattamento dei dati personali, nel rispetto della normativa vigente, di quanto disposto dal presente Regolamento, nonché specificato nell'eventuale disciplinare-programma di cui all'articolo precedente, nonché di ogni altra prescrizione, anche di carattere tecnico, contenuta nei provvedimenti e documenti previsti per il trattamento di dati personali, assicura l'istruzione del personale autorizzato, anche mediante la redazione di disciplinari operativi per l'impiego dei sistemi di videosorveglianza.
2. In particolare, per il sistema di videosorveglianza della sicurezza cittadina, dovranno essere disciplinati, anche con un unico documento, almeno i seguenti aspetti operativi:
    a. l'attività svolta dal personale addetto alla centrale operativa della Polizia locale, autorizzato al trattamento, con particolare riferimento all'impiego dei sistemi di videosorveglianza e agli aspetti connessi, secondo le specifiche del profilo di accesso;
    b. l'attività svolta dal personale della Polizia locale, autorizzato al trattamento, con particolare riferimento alla gestione dei sistemi di videosorveglianza, bodycam, dashcam e UAS, nonché gli aspetti connessi, secondo le specifiche del profilo di accesso ed alle attribuzioni assegnate;
    c. l'impiego di sistemi di videosorveglianza e video-ripresa di cui all'articolo 7, comma 2, del presente Regolamento;
    d. le procedure di accesso alle registrazioni di cui all'articolo 13, del presente Regolamento;
    e. le modalità di impiego di dispositivi di videosorveglianza che integrino funzioni di intelligenza artificiale di cui all'articolo 7-bis, con particolare riferimento alla sorveglianza umana, alla verifica degli esiti prima di ogni atto conseguente, alla gestione dei log e alla segnalazione di malfunzionamenti o incidenti.
3. Gli altri Dirigenti dei Settori/Unità di Staff e/o di Progetto competenti, così come definiti dall'art. 3 del presente Regolamento, possono procedere all'emissione di propri disciplinari operativi secondo le

indicazioni esposte nei commi precedenti, qualora competenti e legittimati all'accesso a specifici impianti di videosorveglianza sul territorio comunale che non siano gestiti dalla Polizia Locale.

Art. 17 – Allegati

1. Le disposizioni del presente Regolamento sono completate dagli allegati al medesimo, i quali ne costituiscono parte integrante.

2. La modifica ovvero la revisione degli allegati è rimessa a specifica Determinazione del Responsabile Designato al trattamento dei dati personali competente, sentito, ove opportuno, il Responsabile per la Protezione dei Dati Personali.

Art. 18 - Disposizioni finali e transitorie

1. Il presente Regolamento entrerà in vigore con il conseguimento dell'esecutività della relativa Deliberazione di Consiglio comunale.

2. Il presente Regolamento abroga ogni disposizione regolamentare precedente in materia di protezione dei dati personali mediante di sistemi di videosorveglianza.

3. Rimangono in ogni caso fatti salvi gli adempimenti di cui all'articolo 4 della Legge 20 Maggio 1970, n. 300, recante "Statuto dei lavoratori" e gli accordi sindacali con le Rappresentanze sindacali in materia.

4. Il presente Regolamento è aggiornato in caso di modifiche della normativa di rango superiore in materia di protezione dei dati personali, Regolamento (UE) 2016/679 e D.lgs. n. 196/2003 e D.lgs. n. 51/2018, e di intelligenza artificiale, ivi compresi gli atti di attuazione del Regolamento (UE) 2024/1689, della Legge n. 132/2025 e del D.lgs. n. 179/2026, nonché la disciplina di cui all'articolo 24, comma 2, lettera h), della Legge n. 132/2025. Per quanto non previsto si rinvia alla normativa vigente e ai provvedimenti del Garante per la protezione dei dati personali.

ALLEGATO Elenco Siti Da Monitorare / Punti Di Installazione Fototrappole

n.	*Area*	*Motivazione*
1	Via Marcigliana	*Via oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
2	Via di Mezza Selva	*Via oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
3	Via delle Foche	*Via oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
4	Via Cento Gocce	*Via oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
5	Via di Fontana Chiusa	*Via oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
6	Via dei Casali	*Via oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
7	Via “Costa” dei Casali	*Via oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
8	Via Fontana Marchetta	*Via oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
9	Via “dei Combattenti”	*Via/Sito oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
10	Via “Forma Immene”	*Via/Sito oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
11	“Cento Gocce”	*Sito oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
12	“Sassi Grossi”	*Sito oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*
13	“Pantano”	*Sito oggetto di costanti fenomeni di abbandono di rifiuti di qualsivoglia natura*

Elenco Siti Da Monitorare / Punti Di Installazione Telecamere

n.	*Area*	*Motivazione*
1	Stazione F.S.	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
2	Via Casilina-Stazione. F.S.	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
3	Via Casilina–Stazione F.S. 2	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
4	Parcheggio Plateatico 1	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
5	Parcheggio Plateatico 2	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
6	Parcheggio Plateatico 3	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
7	Parco “Cerchi” 1	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
8	Parco “Cerchi” 2	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
9	Parco “Cerchi” 3	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
10	Parco “Cerchi” 4	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
11	Piazza del Mercato 1	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
12	Piazza del Mercato 2	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
13	Piazza Mazzini	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
14	Centro Anziani – Attrav. pedonale	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
15	Leonardo da Vinci - Ingresso	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
16	Leonardo da Vinci – Retro	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
17	Parco Tulli	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
18	Prim.M. Iole-Ingres carrabile scuola	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*

19	Prim.M. Iole-Ingr. pedonale scuola	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
20	Prim.M. Iole-Ingresso Via Casilina	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
21	Infanzia F.Pastore-Ingresso	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
22	Infanzia F.Pastore-Parcheggio	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
23	Infanzia Donna Agnese-Cancello	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
24	Infanzia Donna Agnese-Cancello sec.	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
25	Polizia Locale-Uffici	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
26	Polizia Locale-Comandante	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
27	Polizia Locale-Ingresso	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
28	Polizia Locale-Ingresso Comune	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
29	Polizia Locale-Ingresso Vigili	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
30	Vicolo delle Coste-Scala inferiore	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
31	Vicolo delle Coste-Scala superiore	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
32	Fontanone	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
33	Ingresso ex mattatoio	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
34	Via delle Fontana	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
35	Ingresso ex Mattatoio 2	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
36	Retro Via della Fontana	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*
37	Via della Fontana 2	*Polizia Giudiziaria, ambientale e patrimoniale – P.S.*

Elenco Telecamere Lettura Targhe

1	Via Casilina alt. Km 38+400 - dir. Valmontone	*Rilevazione infrazioni CdS – Attività di P.G.*
2	Via Casilina alt. Km 38+400 - dir. Valmontone	*TRED RILEVAZIONE INFRAZIONI ART.146 CDS*
3	Via Casilina alt. Km 38+400 – dir. San Cesareo	*Rilevazione infrazioni CdS – Attività di P.G.*
4	Via Casilina alt. Km 38+400 – dir. San Cesareo	*TRED RILEVAZIONE INFRAZIONI ART.146 CDS*