COMUNE DI CANTELLO

Provincia di Varese

REGOLAMENTO COMUNALE

PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA URBANA INTEGRATA SUL TERRITORIO COMUNALE

Approvato con delibera C.C. n. 30 in data 28/09/2021

Sommario

CAPO I PRINCIPI GENERALI 4
Art. 1 – Oggetto 4
Art. 2 – Definizioni 4
Art. 3 – Finalità del regolamento. 6
Art. 4 – Sistemi di videosorveglianza 6
Art. 5 – Trattamento dei dati personali 6
Art. 6 – Soggetto Designato al trattamento dei dati 7
Art. 7 – Funzioni del Designato 7
Art. 8 – Persone autorizzate ad accedere alla sala di controllo 9
Art. 9 – Soggetti autorizzati al trattamento e dei preposti alla gestione dell'impianto di videosorveglianza 9
CAPO III TRATTAMENTO DEI DATI PERSONALI 10
Art. 10 – Diretta visione delle immagini 10
Art. 11 – Modalità di raccolta e di trattamento dei dati personali 10
Art. 12– Modalità da adottare per i dati video ripresi 11
Art. 13 – Comunicazione 11
Art. 14 – Limiti alla utilizzabilità di dati personali 11
Art. 15 – Tipi di trattamenti autorizzati 12
CAPO IV DIRITTI DEGLI INTERESSATI 12
Art. 16-Informativa 12
Art. 17 – Diritti dell'interessato 13
CAPO V MISURE DI SICUREZZA 13
Art. 18 – Cifratura dei dati trasmessi mediante apparati e tecnologie wireless 13
Art. 19 – Luogo e modalità di memorizzazione delle immagini 13
Art. 20 - Criteri e modalità di estrazione delle immagini 14
Art. 21 – Amministratori di Sistema. 14
Art. 22 – Cessazione del trattamento dei dati 14
Art. 23 – Trasmissione dei video 14
CAPO VI DISPOSITIVI DI VIDEOSORVEGLIANZA 15
Art. 24 – Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada 15
Art. 25 – Utilizzi particolari 15
Art. 26 - Abbandono e conferimento dei rifiuti. 15
Art. 27 - Utilizzo di particolari videocamere mobili (Body Cam e Dash Cam) e Droni. 16
Art. 28 - Foto trappole 16
CAPO VII GESTIONE DEL DATA BREACH 16
Art. 29 – Perdita dei dati – Data Breach 16

Art. 30 – Gestione della comunicazione del Data Breach 16
Art. 31 - Identificazione e indagine preliminare 17
Art 32 – Contenimento, Recovery e risk assessment 17
Art. 33 - Eventuale notifica all'Autorità Garante competente 18
Art. 34 Eventuale comunicazione agli interessati 18
Art. 35 - Documentazione della violazione 18
CAPO VIII TUTELA AMMINISTRATIVA E GIURISDIZIONALE 19
Art. 36 – Tutela 19
Art. 37 – Danni cagionati dal trattamento di dati personali 19
CAPO IX DISPOSIZIONI FINALI 19
Art. 38 – Partenariato pubblico privato per il potenziamento della videosorveglianza ad uso pubblico 19
Art. 39 – Rinvio dinamico 20
Art. 40 – Entrata in vigore 20

CAPO I
PRINCIPI GENERALI

Art. 1 – Oggetto

1. Il presente regolamento disciplina il trattamento dei dati personali realizzato mediante l'impianto di videosorveglianza attivato nel territorio del Comune di Cantello.

2. Per quanto non disciplinato nel presente regolamento, si rinvia alle disposizioni di legge ed in particolare a:

- Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "*Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia*";
- Regolamento UE n. 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;
- Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai 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;
- D.Lgs. 30 giugno 2003, n, 196, come modificato dal D.Lgs. n. 101 del 10 agosto 2018, recante: "Codice in materia di protezione dei dati personali e successive modificazioni;
- D.Lgs. 18/05/2018, 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."
- art. 54 del D.Lgs. 18 agosto 2000, n. 267 e successive modificazioni;
- Decalogo del 29 novembre 2000 promosso dal Garante per la protezione di dati personali;
- Circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/A/471;
- D.L. 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 ", ed in particolare dall'art. 6;
- D.L. 20 febbraio 2017 n 14 recante "Disposizioni urgenti in materia di sicurezza delle città"
- "Provvedimento in materia di videosorveglianza" emanato dal garante per la protezione dei dati personali in data 8 aprile 2010.

Art. 2 – Definizioni

1. Ai fini del presente regolamento si intende:

a) per «dato personale», 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 a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online

o un riferimento a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) per «trattamento», 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;

c) per «profilazione», qualsiasi forma di trattamento automatizzato di informazioni per valutare determinati aspetti personali per analizzare o prevedere dati riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di una persona;

d) per «pseudonimizzazione», il trattamento di dati personali in modo tale che gli stessi non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e siano soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

e) per «titolare del trattamento», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili per la sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

f) per «responsabile del trattamento», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

g) per «incaricato del trattamento», la persona fisica che abbia accesso a dati personali;

h) per "interessato", la persona fisica identificata o identificabile a cui si riferiscono i dati personali oggetto di trattamento;

i) per «terzo», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

j) per «violazione dei dati personali», la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

k) per «comunicazione», dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

l) per "diffusione", dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) per "dato anonimo", il dato che in origine o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Art. 3 – Finalità del regolamento.

1. Il presente regolamento garantisce che il trattamento dei dati personali effettuato mediante i sistemi di videosorveglianza gestiti dal Comune di Cantello - Comando di Polizia Locale – compresi quelli collegati alle Forze dell'Ordine, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, ai sensi delle vigenti disposizioni in materia di protezione di dati personali.

Art. 4 – Sistemi di videosorveglianza

1. Il sistema di videosorveglianza comunale è costituito da una serie di postazioni di ripresa fisse collegate attraverso ponti radio o cavo alla centrale operativa della Polizia Locale e alle Forze dell'Ordine; postazioni mobili, body cam e dash cam[1].

2. Il sistema può essere implementato mediante sistemi integrati, sistemi intelligenti e sistemi per rilevare violazioni al codice della strada.[2]

3. L'utilizzo dei sistemi di cui ai commi precedenti è conforme alle funzioni istituzionali riconosciute al Comune di Cantello in forza di disposizioni di legge[3], nonché dallo statuto e dai regolamenti comunali. La disponibilità tempestiva di immagini presso il Comando della Polizia Locale e delle Forze dell'Ordine costituisce uno strumento di prevenzione e di razionalizzazione dell'azione dei predetti organi di polizia locale e statale.

Art. 5 – Trattamento dei dati personali

1. Il trattamento dei dati personali è effettuato a seguito dell'attivazione dei sistemi di videosorveglianza.

2. Il trattamento dei dati attraverso l'attività di videosorveglianza è effettuato ai fini di:

- tutelare la pubblica sicurezza in ambito comunale;
- vigilare in materia di sicurezza urbana, sulla corretta osservanza di ordinanze e/o regolamenti comunali, consentire l'accertamento di illeciti di natura penale e/o amministrativa;
- vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
- monitorare i flussi di traffico lungo le strade e l'accesso alle aree pedonali e alle zone a traffico limitato;
- fornire uno strumento operativo per finalità di protezione civile.

3. La ripresa delle immagini viene effettuata con una bassa risoluzione nel caso di impiego di telecamere per il controllo del traffico e in tutti i casi in cui è sufficiente una ripresa di contesto. La ripresa delle immagini viene effettuata con un'alta risoluzione per finalità di pubblica sicurezza e sicurezza urbana[4].

4. Nelle scuole gli impianti sono attivati esclusivamente negli orari di chiusura degli edifici.

---

[1] definizione di body cam: microcamera da apporre sull'uniforme; - definizione dash cam: telecamera applicabile sul parabrezza dei veicoli al fine di registrare gli eventi che accadono all'esterno della vettura.

[2] Sistemi integrati: sistemi collegati con le FF.OO.; Sistemi intelligenti: sistemi con TLC che monitorano una determinata area e restituiscono dati statistici quali, per esempio, il numero di presenze; sistemi per rilevare le violazioni al codice della strada da remoto e in automatico: sistemi per il controllo degli accessi alle AP/ZTL ovvero per la rilevazione del passaggio al semaforo con il rosso, per la rilevazione della velocità o del sorpasso in aree vietate.

[3] In particolare dal D.Lgs. 18 agosto 2000 n. 267, dal D.P.R. 24 luglio 1977, n. 616, dal D.Lgs. 31 marzo 1998, n. 112, dalla legge 7 marzo 1986 n. 65.

[4] Direttiva Ministero dell'Interno 2 marzo 2012.

5. Il sistema di videosorveglianza comporta il trattamento di dati personali rilevati mediante le riprese delle videocamere e che, in relazione ai luoghi di installazione, interessano tutti coloro che transitano nell'area interessata.

6. Gli impianti di videosorveglianza non possono essere utilizzati[5] per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale.

CAPO II
SOGGETTI DEL TRATTAMENTO

Art. 6 – Soggetto Designato al trattamento dei dati

1. Il Comandante della Polizia Locale Responsabile del servizio è individuato quale Designato del trattamento dei dati personali rilevati, ai sensi e per gli effetti dell'art. 2-quaterdecies del D.Lgs. n. 196/2003 come novellato dal D.Lgs. n. 101/2018.

2. La nomina è effettuata con atto del Sindaco, nel quale sono analiticamente specificati i compiti affidati al Designato.

3. Il Designato deve rispettare pienamente quanto previsto in tema di trattamento dei dati personali dalle leggi vigenti, ivi incluso il profilo della sicurezza e dalle disposizioni del presente regolamento.

4. Il Designato procede al trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni impartite in sede di nomina.

5. I compiti affidati al Designato devono essere analiticamente specificati per iscritto, in sede di designazione.

6. Il Designato custodisce le chiavi per l'accesso ai locali della centrale di controllo, le chiavi degli armadi per la conservazione delle immagini, nonché le parole chiave per l'utilizzo dei sistemi.

Art. 7 – Funzioni del Designato

1. Il Designato:

- individua e nomina con propri atti i soggetti Autorizzati al trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29 del REG. 2016/679 U.E. nonché all'art 18 del D.Lgs 51/2018. Detti soggetti saranno opportunamente istruiti e formati da parte del Designato del trattamento con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati. La gestione degli impianti di videosorveglianza e dei sistemi di lettura targhe è riservata agli operatori della Polizia Locale aventi qualifica di Ufficiali e Agenti di polizia giudiziaria ai sensi dell'art. 55 del c.p.p.

- verifica e controlla che il trattamento dei dati effettuato mediante sistema di videosorveglianza sia realizzato nel rispetto dei principi di cui all'art. 5 del REG. 2016/679 U.E. nonché all'art 3 del D.Lgs 51/2018 e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente; garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;

[5] art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970 e successive modificazioni)

- tenuto conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto, delle finalità del trattamento e in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adotta tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del REG. 2016/679 U.E.; nonché dell'art. 25 del D.Lgs 51/2018

- assiste il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del REG. 2016/679 U.E.;

- assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza, mettendo in atto misure tecniche e organizzative adeguate, in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, tenuto conto anche delle segnalazioni del D.P.O.;

- garantisce l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile nei confronti dell'Ente della formale e tempestiva formulazione della proposta di adozione delle misure necessarie;

- assicura l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;

- assiste il Titolare nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del REG. 2016/679 U.E.;

- assiste il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del REG. 2016/679 U.E. e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del REG. 2016/679 U.E.;

- affianca il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del REG. 2016/679 U.E., nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico;

- garantisce che il Responsabile della Protezione dei Dati designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;

- mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;

- è responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta

- assicura che i soggetti autorizzati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali.

- garantisce la tempestiva emanazione di direttive scritte al personale autorizzato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto con il Responsabile della Protezione dei dati.

Art. 8 – Persone autorizzate ad accedere alla sala di controllo

1. L'accesso alla sala di controllo è consentito solamente al personale in servizio della Polizia Locale autorizzato per iscritto dal Comandante e agli autorizzati addetti ai servizi, di cui ai successivi commi.

2. Eventuali accessi di persone diverse da quelli innanzi indicate devono essere autorizzati per iscritto dal Comandante della Polizia Locale.

3. Possono essere autorizzati all'accesso solo incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità di cui al presente regolamento, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali e il personale delle forze dell'ordine.

4. Il Designato impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.

5. I soggetti di cui al presente articolo hanno obbligo del puntuale rispetto delle istruzioni e della corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art. 9 – Soggetti autorizzati al trattamento e dei preposti alla gestione dell'impianto di videosorveglianza

1. Il Comandante della Polizia Locale in qualità di soggetto Designato, individua i soggetti autorizzati al trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza. L'autorizzazione è effettuata con atto scritto, nel quale sono analiticamente specificati i compiti affidati ai soggetti autorizzati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati. I soggetti autorizzati sono individuati tra gli appartenenti al Corpo di Polizia Locale che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

2. In particolare, i soggetti autorizzati devono:

- per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento, anche temporaneo, dal posto di lavoro;

- custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;

- non creare banche dati nuove senza autorizzazione espressa del Designato;

- fornire al Titolare ed al Responsabile della Protezione dei dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

3. I soggetti autorizzati devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Titolare o del Designato.

4. L'utilizzo degli apparecchi di ripresa da parte dei soggetti autorizzati al trattamento deve essere conforme ai limiti indicati dal presente Regolamento e alle disposizioni vigenti.

5. Gli Autorizzati, fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati possono riesaminare le registrazioni, nel limite del tempo ammesso per la conservazione di cui all'articolo 11, solo in caso di effettiva necessità per il conseguimento delle finalità di cui agli artt. 3 e 5.

6. La mancata osservanza degli obblighi previsti al presente articolo comporta l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.

CAPO III
TRATTAMENTO DEI DATI PERSONALI

Art. 10 – Diretta visione delle immagini

1. La diretta visualizzazione delle immagini rilevate con i sistemi di videosorveglianza nella centrale operativa è limitata ad obiettivi particolarmente sensibili e strategici per la pubblica sicurezza e la sicurezza urbana.

2. Il Designato e gli Autorizzati si obbligano a non effettuare riprese di dettaglio dei tratti somatici delle persone che non siano funzionali alle finalità istituzionali perseguite tramite l'attivazione dell'impianto.

3. Le Forze dell'Ordine per finalità proprie e previo accordo con il Titolare, possono essere collegate con i sistemi di rilevazione.

Art. 11 – Modalità di raccolta e di trattamento dei dati personali

1. L'installazione delle telecamere avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili) in conformità all'elenco dei siti di ripresa predisposto dall'Amministrazione Comunale.

2. L'attività di videosorveglianza deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, limitando l'angolo di visuale delle riprese.

3. Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali perseguite tramite l'attivazione dell'impianto. I segnali video delle unità di ripresa sono inviati presso la sede del Corpo di Polizia Locale o datacenter dove sono registrati su appositi server. I video possono essere visionati dalle Forze dell'ordine a ciò autorizzate dal Titolare o dal Designato.

5. I dati personali oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza;

- raccolti e registrati per le finalità di cui all'art. 3 del presente Regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;

- raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.

6. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata al massimo a 7 giorni, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché qualora si debba aderire ad una specifica richiesta investigativa di polizia giudiziaria.

7. Nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della pubblica sicurezza (rif. Direttiva 2016_680 EU e D.Lgs 51/2018), alla luce delle richiamate disposizioni normative, il termine massimo di durata della conservazione è definito a seconda dello scenario concreto, fatte salve specifiche esigenze di ulteriore conservazione.

8. Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

9. In caso di cessazione del trattamento, i dati personali sono distrutti.

Art. 12– Modalità da adottare per i dati video ripresi

1. I monitor degli impianti di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.

2. L'accesso alle immagini da parte del Designato e degli Autorizzati al trattamento si limita alle attività oggetto della sorveglianza; eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione.

3. Nel caso in cui le immagini siano conservate, i relativi supporti devono essere crittografati e custoditi per l'intera durata della conservazione, in un armadio o simile struttura dotato di serratura, apribile solo dal Designato e dagli Autorizzati al trattamento dei dati.

4. La cancellazione delle immagini è garantita mediante gli strumenti e le procedure tecnologiche più avanzate.

5. Nel caso in cui il supporto di registrazione debba essere sostituito per eccessiva usura, lo stesso è distrutto in modo da renderlo inutilizzabile e non permettere il recupero dei dati in esso presenti.

6. Tutti gli accessi alla visione devono essere documentati e registrati tramite sistema automatico di log.

Art. 13 – Comunicazione

1. La comunicazione dei dati personali da parte dell'Ente a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa esclusivamente per lo svolgimento di compiti di interesse pubblico e per finalità istituzionali (art. 2 ter del D.Lgs. n. 196/03).

2. È in ogni caso fatta salva la comunicazione o diffusione di dati richiesti in conformità alla legge, da forze di polizia, dall'autorità giudiziaria o da altri soggetti pubblici.

Art. 14 – Limiti alla utilizzabilità di dati personali

1. I dati personali trattati in violazione della disciplina in materia di trattamento dei dati personali non possono essere utilizzati ai sensi dell'art. 2 decies del D.Lgs. n. 196/03, salvo quanto previsto dall'art. 160 bis dello stesso decreto[6].

[6] Art. 160 bis (Validità, efficacia e utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento). La validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali.

Art. 15 – Tipi di trattamenti autorizzati

1. Con l'installazione e l'esercizio del sistema di videosorveglianza sono autorizzati esclusivamente le seguenti tipologie di trattamenti:

- creazione e gestione di gruppi e profili di utenti;
- consultazione immagini live da telecamera;
- messa a fuoco e brandeggiamento della telecamera;
- impostazione di limiti al brandeggiamento delle telecamere;
- impostazione di zone oscurate staticamente;
- registrazione di immagini;
- cancellazione di immagini;
- consultazione immagini registrate;
- estrazione (duplicazione) immagini registrate;
- definizione aree di motion-detection[7];
- definizione azioni da eseguire in concomitanza di eventi di motion-detection;
- accensione di sorgenti luminose o ad infrarosso;
- rilevazione e inventario degli indirizzi ip presenti in rete;
- rilevazione e inventario dei mac address presenti in rete;
- installazione e configurazione di software applicativo;
- installazione e configurazione di software di base;
- installazione di "patch" e "hot fix";
- attivazione collegamenti da remoto;
- interventi generici di manutenzione e configurazione hardware e software
- attivazione e configurazione di meccanismi di tracciatura ("logging");
- estrazione e conservazione di files di log;
- apposizione di firma digitale qualificata e di marcatura temporale e files di log;
- apposizione di firma digitale qualificata e marcatura temporale ad immagini e sequenze filmiche.

CAPO IV
DIRITTI DEGLI INTERESSATI

Art. 16-Informativa

1. I soggetti interessati, che stanno per accedere o che si trovano in una zona videosorvegliata, devono essere informati mediante appositi cartelli conformi ai modelli approvati dall'Autorità Garante per la protezione dei dati personali.

2. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, sono installati più cartelli.

3. Sul sito istituzionale del Comune è pubblicata l'informativa completa contenente le modalità e le finalità degli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso dell'interessato secondo quanto previsto dal Regolamento UE 2016/679 e dal D.Lgs. n. 51/2018.

[7] motion-detection: attivazione della ripresa al solo verificarsi di un prestabilito evento, per esempio il movimento di una persona

Art. 17 – Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, previa presentazione di apposita istanza, ha diritto:

a) di conoscere l'esistenza del trattamento di dati che lo riguardano;

b) di essere informato sugli estremi identificativi del Titolare e del Designato al trattamento, oltre che sulle finalità e modalità del trattamento dei dati;

c) di ottenere:

- la conferma dell'esistenza o meno di dati personali che lo riguardano;

- la trasmissione in forma intelligibile dei dati che lo riguardano e della loro origine;

- l'informazione sulle procedure adottate in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento;

- la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati.

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

3. Per ciascuna delle richieste di cui al comma 1, lett. c), può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati ~~e~~ comprensivi dei costi del personale.

4. 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.

5. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.

6. Le istanze di cui al presente articolo possono essere trasmesse al Titolare o al Designato anche mediante lettera raccomandata o posta elettronica.

CAPO V
MISURE DI SICUREZZA

Art. 18 – Cifratura dei dati trasmessi mediante apparati e tecnologie wireless

1. I dati trasmessi mediante apparati wireless devono essere cifrati al fine di garantirne la riservatezza.

Art. 19 – Luogo e modalità di memorizzazione delle immagini

1. Le immagini riprese dalle telecamere devono essere memorizzate in formato elettronico su un unico o su un numero limitato di supporti di memorizzazione di massa centralizzati e collocati all'interno di un unico apparato di tipo "server". È fatta salva la necessità di una memorizzazione "di backup" anche su un server remoto. Il suddetto server deve essere dedicato esclusivamente alla memorizzazione delle immagini registrate dalle telecamere del sistema di videosorveglianza e non deve essere dedicato ad altri scopi. Il server non deve essere collegato alla rete internet. È fatta salva

la possibilità di collegamento, previa autorizzazione scritta da parte del Titolare, limitatamente a casi e per finalità specifiche e ben individuate, per intervalli di tempo il più possibile contenuti.
2. Non è consentita la memorizzazione delle immagini in locale a livello di postazione "client" o comunque su supporti e strumenti diversi dal server centralizzato. Nei soli casi in cui si evidenzi la necessità di una conservazione preventiva di immagini, la loro memorizzazione temporanea è consentita solamente in aree appositamente dedicate del server e la loro cancellazione deve avvenire non appena possibile.

Art. 20 - Criteri e modalità di estrazione delle immagini

1. L'estrazione di immagini o di intere riprese mediante duplicazione a favore delle Forze dell'Ordine o dell'Autorità Giudiziaria è consentita previa richiesta scritta da parte degli organi anzidetti e di autorizzazione scritta del Titolare o del Designato.
2. La richiesta di estrazione deve specificare chiaramente il luogo o la telecamera di registrazione e l'intervallo temporale da estrarre e collocare su supporto esterno di memorizzazione.

3. Il sistema appone l'impronta digitale su ciascun frame delle registrazioni delle immagini video, a garanzia della conformità della copia.

4. All'atto della consegna del supporto di memorizzazione contenente le immagini estratte, l'incaricato della consegna deve far firmare e trattenere apposito documento attestante la consegna e la ricevuta delle immagini estratte.

5. Le operazioni di cui sopra sono annotate su apposito registro informatico riportante anche giorno, data e ora di effettuazione delle operazioni.

6. Per accelerare i tempi di indagine, previa stipula di una convenzione / accordo interforze, le FF.OO. possono accedere remotamente in via telematica al sistema di videosorveglianza.

7. Gli accessi dovranno avvenire su base nominativa individuale e dovranno venire tracciati (log).

Art. 21 – Amministratori di Sistema.

1. I soggetti che svolgono mansioni di Amministratore di sistema sono individuati dal Titolare del trattamento.
2. L'accesso al server da parte dell'Amministratore di Sistema avviene nel rispetto delle disposizioni di legge.

Art. 22 – Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono:

a) distrutti;

b) conservati per fini esclusivamente istituzionali dell'impianto attivato in conformità a quanto previsto dal Regolamento UE 2016/679 relativo alla protezione dei dati e dall'art. 2 del D.Lgs. 51/2018 relativo 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.

Art. 23 – Trasmissione dei video

1. Al fine di garantire la sicurezza della trasmissione dei dati, gli stessi sono comunicati adottando le opportune misure di sicurezza volta alla tutela del dato.

CAPO VI
DISPOSITIVI DI VIDEOSORVEGLIANZA

Art. 24 – Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada

1. Gli impianti elettronici di rilevamento automatizzato delle infrazioni, utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale, analogamente all'utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.

2. L'utilizzo di tali sistemi è lecito se sono raccolti solo dati pertinenti e non eccedenti al perseguimento delle finalità istituzionali del Titolare; a tal fine deve essere delimitato ~~e~~ l'angolo visuale delle riprese per non raccogliere immagini non pertinenti o inutilmente dettagliate.

3. Si osservano le seguenti specifiche disposizioni contenute nelle disposizioni di settore:

- le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la redazione del verbale di accertamento delle violazioni (es. ai sensi dell'art. 383 del D.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento amministrativo (es. pedoni, altri utenti della strada);
- le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;
- le fotografie o le immagini che costituiscono fonte di prova per le violazioni contestate non devono essere inviate d'ufficio al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;
- in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e di ottenere dalla Polizia Locale ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.

Art. 25 – Utilizzi particolari

1. Qualora il sistema di videosorveglianza venga utilizzato a fini di rilevazione degli accessi dei veicoli ai centri storici, alle corsie riservate e alle zone a traffico limitato o aree pedonali, si deve rispettare quanto stabilito dalle disposizioni vigenti in materia[8].
2. I dati trattati potranno essere conservati solo per il periodo necessario per contestare le infrazioni e definire il contenzioso e si potrà accedere ad essi solo a fini di polizia stradale o di polizia giudiziaria.

Art. 26 - Abbandono e conferimento dei rifiuti.

1. In applicazione dei principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza fissi e/o mobili è consentito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e/o di sostanze pericolose

[8] D.P.R. 22 giugno 1999, n. 250

laddove non risulti possibile o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.
2. Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito laddove risultano inefficaci o inattuabili altre misure, nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente.

Art. 27 - Utilizzo di particolari videocamere mobili (Body Cam e Dash Cam) e Droni.

1. Per specifiche finalità concernenti la tutela dell'ordine, della sicurezza pubblica e urbana, la prevenzione, l'accertamento e la repressione dei reati, gli operatori di Polizia Locale sono dotati di sistemi di microtelecamere da indossare sulla divisa nonché da installare all'interno del parabrezza del veicolo in dotazione.

2. Il trattamento dei dati personali effettuati con tali sistemi di ripresa devono rispettare i principi di cui all'art. 5 del Regolamento UE 2016/679 e della Direttiva UE 2016/680.

3. I dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati; devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali sono stati raccolti o successivamente trattati.

4. Gli operatori di Polizia Locale abilitati al trattamento di dati possono utilizzare le riprese effettuate tramite droni per visualizzare aree non facilmente accessibili o per avere una visione aerea dello scenario operativo. Qualora non sussistano finalità di sicurezza o necessità di indagine previste da disposizioni di legge che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione di adeguata cartellonistica per l'informativa agli utenti frequentatori di dette aree.

Art. 28 - Foto trappole

Gli apparati "Telecamere modulari" (foto trappole) vengono posizionati esclusivamente nei luoghi teatro di illeciti penali o amministrativi, quando questi ultimi non siano altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza o necessità di indagine che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica per l'informativa agli utenti frequentatori di dette aree.

CAPO VII
GESTIONE DEL DATA BREACH

Art. 29 – Perdita dei dati – Data Breach

1. Il personale Autorizzato che provvede al concreto utilizzo dei dispositivi di videosorveglianza deve segnalare immediatamente al Designato o al Titolare qualsiasi anomalia, malfunzionamento, nonché la perdita – anche parziale – accidentale o volontaria di dati (Data Breach).

Art. 30 – Gestione della comunicazione del Data Breach

1. Le violazioni di dati personali sono gestite dal Titolare del trattamento o dal Designato sotto la supervisione del Responsabile della protezione dei dati dell'incidente verificatosi (DPO).

2. In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, sussiste l'obbligo in capo ad ogni soggetto abilitato al trattamento di dati di rendere tempestiva comunicazione al Designato e al Titolare mediante compilazione di apposito modulo al fine di affrontare immediatamente la situazione per minimizzare l'impatto della violazione e prevenire che si ripeta.

3. Il Titolare del trattamento o il Designato informano tempestivamente e con il mezzo più idoneo il Responsabile della protezione dei dati dell'incidente verificatosi.

Art. 31 - Identificazione e indagine preliminare

1. Il Titolare del trattamento insieme al Responsabile della protezione dei dati conducono una valutazione iniziale dell'incidente occorso al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) o se sia necessaria un'indagine più approfondita dell'accaduto. A tal fine coinvolgono anche l'Amministratore di sistema.
2. La valutazione iniziale è effettuata attraverso l'esame delle seguenti informazioni riportate nel modulo di segnalazione:

- data di scoperta della violazione (tempestività);
- soggetto che è venuto a conoscenza della violazione;
- descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- categorie e numero approssimativo degli interessati coinvolti nella violazione;
- descrizione di eventuali azioni già attuate.

Art 32 – Contenimento, Recovery e risk assessment

1. Il Titolare del trattamento o il Designato insieme al Responsabile della protezione dei dati stabiliscono:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (es. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- una volta identificate le azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

2. Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il Responsabile della protezione dei dati valutano la gravità della violazione utilizzando il Modulo di valutazione del Rischio connesso al Data Breach che dovrà essere esaminato tenendo in debita considerazione i principi e le indicazioni di cui all'art. 33 del Regolamento UE 2016/679.

3. Se la violazione comporta un rischio elevato per i diritti delle persone, il Titolare deve rendere adeguata informazione a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Art. 33 - Eventuale notifica all'Autorità Garante competente

1. Qualora si debba effettuare la notifica della violazione dei dati all'Autorità Garante il Titolare deve provvedervi senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza.

2. Il Titolare del trattamento invia il modulo di notifica all'Autorità Garante per la protezione dei dati personali così da effettuare la notificazione del Data Breach[9].

Art. 34 Eventuale comunicazione agli interessati

1. La comunicazione della violazione dei dati agli interessati deve contenere:
   - il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
   - la descrizione delle probabili conseguenze della violazione dei dati personali;
   - la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

3. La comunicazione è effettuata tramite e-mail, SMS o messaggi diretti. Solo qualora non sia possibile effettuare una comunicazione diretta si effettuerà una comunicazione pubblica idonea a raggiungere l'interessato.

Art. 35 - Documentazione della violazione

1. Ogni qualvolta si verifichi un incidente l'Ente è tenuto a documentarlo mediante la tenuta del Registro dei Data Breach contenente le seguenti informazioni:

(i) n. violazione; (ii) data violazione; (iii) natura della violazione; (iv) categoria di interessati; (v) categoria di dati personali coinvolti; (vi) numero approssimativo di registrazioni dei dati personali; (vii) conseguenze della violazione; (viii) contromisure adottate; (ix) se sia stata effettuata notifica all'Autorità Garante Privacy; (x) se sia stata effettuata comunicazione agli interessati.

2. La documentazione è affidata al Titolare del trattamento o al Designato che vi provvede con l'ausilio dell'Amministratore di Sistema

3. Il Registro dei Data Breach deve essere costantemente aggiornato e messo a disposizione dell'Autorità per consentire di effettuare eventuali verifiche sul rispetto della normativa.

[9] I modelli sono reperibili sul sito del Garante per la protezione dei dati personali o al link: https://servizi.gpdp.it/databreach/s/

CAPO VIII
TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 36 – Tutela

1. Per quanto attiene al diritto di proporre reclamo o segnalazione all'Autorità Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente alle disposizioni vigenti[10].

Art. 37 – Danni cagionati dal trattamento di dati personali

1. Chiunque subisce un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile del trattamento esterno.

2. Il Titolare e il Responsabile del trattamento sono esonerati dalla responsabilità se dimostrano che l'evento dannoso non in alcun modo a loro imputabile.

3. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti.

CAPO IX
DISPOSIZIONI FINALI

Art. 38 – Partenariato pubblico privato per il potenziamento della videosorveglianza ad uso pubblico

1. Il Comune promuove ed attua il coinvolgimento dei privati per la realizzazione di punti di videosorveglianza orientati comunque su vie ed aree pubbliche, nel rispetto dei principi di cui al presente Regolamento.

2. I privati interessati assumono ogni onere per:

- acquistare le attrezzature e renderle operative, con connessione al sistema centrale ovvero con memorizzazione locale delle immagini in conformità alle caratteristiche tecniche dell'impianto comunale o di un modello compatibile;

- metterle a disposizione del Comune a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa.

3. Il Comune assume la responsabilità della gestione dei dati raccolti; nonché gli oneri per la manutenzione periodica dell'impianto, salvo diversi accordi tra le parti.

4. In accordo con il Comune e mediante la stipula di apposita convenzione i soggetti privati che hanno ceduto i propri impianti di videosorveglianza al Comune possono decidere di affidare il controllo diretto delle telecamere a istituti di vigilanza privata anche prevedendo l'installazione dell'impianto presso una *controll room* dedicata collegata con la Centrale Operativa della Polizia Locale. Gli oneri finanziari dell'affidamento di tale servizio ricadono sul soggetto privato che una volta individuato l'istituto di vigilanza privata cui affidare il servizio ne comunicherà il nominativo al Comune.

---

[10] Alla data di stesura del presente regolamento, in particolare gli artt. 77 e ss, REG. 2016/679 U.E. e le disposizioni attuative.

5. Spetterà poi al Comune, in qualità di Titolare del trattamento dati derivanti dal sistema di videosorveglianza, procedere ai sensi di legge a tutti gli atti conseguenti ivi compresa l'attribuzione della funzione di Autorizzato al trattamento dati.

Art. 39 – Rinvio dinamico

1. Le disposizioni del presente regolamento si intendono modificate per effetto di sopravvenute norme vincolanti europee, statali e regionali. Pertanto, in attesa della formale modificazione del presente regolamento, si applica la normativa sovraordinata.

Art. 40 – Entrata in vigore

1. Il presente Regolamento entra in vigore con il conseguimento della esecutività della deliberazione di approvazione.

2. Si intende abrogata ogni disposizione regolamentare in contrasto con il presente regolamento.