REGOLAMENTO PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA NEL TERRITORIO COMUNALE

Approvato con Delibera del Consiglio Comunale n. 7 del 20/03/2024

in vigore dal 7/04/2024

Indice

Articolo 1 – Premessa

Il presente regolamento disciplina le modalità di raccolta, trattamento e conservazione dei dati personali mediante sistemi di videosorveglianza gestiti, nell'ambito del proprio territorio, dal Comando di Polizia Locale del Comune.
Il trattamento dei dati personali è effettuato a seguito dell'attivazione di sistemi di videosorveglianza che fanno uso di telecamere fisse e/o mobili.

Un sistema di videosorveglianza è costituito da dispositivi analogici e digitali nonché da software per l'acquisizione di immagini al fine di gestirle e mostrarle a uno o più operatori.
I suoi componenti sono così riassumibili:

1) Ambiente video per l'acquisizione delle immagini, le interconnessioni e la gestione delle immagini:

- le immagini vengono acquisite in un formato tale da poter essere utilizzate dal resto del sistema;
- le interconnessioni comprendono tutte le trasmissioni di dati all'interno dell'ambiente video, intese per connessioni con cavi, reti digitali e trasmissioni wireless, mentre le comunicazioni descrivono tutti i segnali video e dati di controllo, digitali o analogici;
- la gestione delle immagini comprende l'analisi, la conservazione e la presentazione di un'immagine o di una sequenza di immagini.

2) Funzioni logiche, connesse alla gestione del sistema, che comprende:

- gestione dei dati e delle attività, comprendente la gestione dei comandi degli operatori e delle attività generate dal sistema (procedure di allarme, operatori di allarme);
- le interfacce con altri sistemi che potrebbero includere la connessione ad altri sistemi di sicurezza (controllo accessi, allarme antincendio) anche non legati alla sicurezza (sistemi di gestione edifici, riconoscimento automatico delle targhe).

3) La sicurezza del sistema di videosorveglianza, che consiste nella riservatezza, nell'integrità e nella disponibilità del sistema e dei dati; comprende la sicurezza fisica di tutti i componenti ed il controllo dell'accesso al sistema di videosorveglianza; la sicurezza dei dati comprende la prevenzione della perdita o della manipolazione dei dati.

Nel regolamento, per sistema di videosorveglianza si intende un complesso di strumenti, come anzi descritti, finalizzati alla vigilanza in remoto mediante dispositivi di ripresa video per la captazione di immagini, ed eventuale conseguente analisi, collegati ad un centro di controllo e coordinamento direttamente gestito dal Comando di Polizia Locale.

Il presente regolamento è finalizzato a garantire che il trattamento dei dati personali, effettuato mediante i sistemi di videosorveglianza installati, manutenuti e gestiti dal Comune:

a. si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale;
b. siano adottate tutte le misure tecniche e organizzative al fine di garantire, in particolare, il principio della minimizzazione dei dati riducendo quindi al minimo l'utilizzo dei dati personali.

L'utilizzo dei dati personali, nell'ambito definito dal presente regolamento, non necessita del consenso degli interessati in quanto viene effettuato per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri o necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento.

Articolo 2 – Norme di riferimento e principi generali

Norme di riferimento

1. Per tutto quanto non dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto da:

- 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 di seguito RGPD);
- 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;
- 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. 18 maggio 2018, n. 51 – Attuazione della Direttiva UE 2016/680 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";
- D.P.R. n. 15 del 15.01.2018, recante "Regolamento a norma dell'art. 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";
- Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008);

- Legge n. 38/2009 recante “misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori”;
- Circolare dell'11 settembre 2020 - “Disposizioni urgenti in materia di sicurezza delle città” convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48. Patti per l’attuazione della sicurezza urbana e installazione di sistemi di videosorveglianza;
- Art. 54 del D.Lgs. 18 agosto 2000, n. 267 e successive modificazioni;
- Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell’8 aprile 2010 (G.U. n. 99 del 29/04/2010);
- Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato Europeo per la protezione dei dati (European Data Protection Board);
- Art.5 del decreto-legge 20 febbraio 2017, n.14 convertito con modificazioni dalla legge 18 aprile 2017, n.48.

2. I dati personali raccolti per l’esecuzione di un compito di autorità per le finalità di prevenzione, indagine, accertamento e perseguimento di reati sono trattati nel rispetto dei principi dell’art.3 del D.Lgs. 51/2018, e:

- per le limitazioni alla raccolta dei dati e per la loro cancellazione è applicato l’art. 12 del D.Lgs. 51/2018;
- per il diritto di accesso ai dati ed alle immagini personali l’art. 11 del D.Lgs. 51/2018;
- per la conservazione dei dati l’arti. 4 del D.Lgs. 51/2018.

3. I dati personali raccolti per l’esecuzione dei compiti di interesse pubblico o connessi all’esercizio di pubblici poteri diversi da quelli del punto precedente di cui è investito il Titolare del trattamento sono trattati nel rispetto dei principi dell’art.5 del Reg. UE/2016/679, e:

- per le limitazioni alla raccolta dei dati e la loro cancellazione sono applicati gli articoli 18 e 17 del Reg. UE/2016/679;
- per il diritto di accesso ai dati ed alle immagini personali l’art. 15 del Reg. UE/2016/679;

Principi generali

4. L’utilizzo dei sistemi di videosorveglianza viene attuato attraverso un corretto impiego delle applicazioni e nel rispetto dei principi applicabili al trattamento di dati personali di cui all’art. 5 dell’RGPD:

a. liceità, quale rispetto della normativa: 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 i Comuni e il Comando di Polizia Locale sono investiti;
b. proporzionalità, con sistemi attuati con attenta valutazione: 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 quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento;

c. finalità, attuando il trattamento dei dati solo per scopi determinati ed espliciti. È consentita la videosorveglianza come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno 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.;

d. necessità, con esclusione di uso superfluo della videosorveglianza: 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.

Articolo 3 – Definizioni

1. Ai fini del presente regolamento, si intende:

a. per "banca di dati", il complesso di dati personali, formatosi presso la sala di controllo e trattato esclusivamente mediante riprese video o foto che, in relazione ai luoghi di installazione delle videocamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;

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 "dato personale", qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere individuata, direttamente o indirettamente, attraverso un nominativo, un numero, 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;

d. per "Titolare del trattamento" il Comune, nella persona del Sindaco pro-tempore, cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali;

e. per "responsabile interno", la persona fisica legata da rapporto di lavoro al Titolare, che opera sotto la sua autorità e designata dal medesimo allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003;

f. per “Responsabile del trattamento”, ai sensi dell’art. 28 GDPR, 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 “autorizzati”, le persone fisiche che operano sotto l’autorità diretta del titolare o del responsabile del trattamento;

h. per “interessato”, la persona fisica che può essere identificata o identificabile, a cui si riferiscono i dati personali;

i. per “comunicazione”, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, in qualunque forma, anche mediante la loro messa a disposizione, consultazione, o mediante interconnessione;

j. per “diffusione” la messa a conoscenza generalizzata dei dati personali in qualunque forma, anche mediante la messa a disposizione o consultazione a soggetti indeterminati;

k. per “dato anonimo”, il dato che “ab origine”, a seguito di inquadratura o di trattamento non può essere associato ad un interessato identificato o identificabile;

l. per “limitazione”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

Articolo 4 – Finalità degli impianti

1. Le finalità di utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono relative alle funzioni istituzionali demandate ai Sindaci ed ai Comuni:

a. dal decreto-legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 “disposizioni urgenti in materia di sicurezza delle città”;

b. dal D.Lgs. 18 agosto 2000, n. 267, dal D.P.R. 24 luglio 1977, n. 616;

c. dalla legge sull’ordinamento della Polizia Locale 7 marzo 1986, n. 65 nonché dallo Statuto Comunale e dai Regolamenti Comunali vigenti;

In particolare, il trattamento dei dati è finalizzato a:

a) alla tutela della sicurezza urbana, intesa, secondo la definizione del Decreto del Ministero dell’Interno del 5 agosto 2008 riformulata dall’art. 4 del D.L. 20 febbraio 2 2017, n. 14, convertito, con modificazioni, nella 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 o patti locali ispirati ad una logica di gestione consensuale ed integrata della sicurezza;

b) svolgere attività di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché a rafforzare la cooperazione giudiziaria in materia penale e di polizia;

c) rilevare e controllare le targhe dei veicoli in transito attraverso telecamere in grado di leggere le targhe e trasformarle in una stringa alfanumerica, al fine di poter disporre di utili elementi per l'avvio di eventuali accertamenti connessi con la sicurezza urbana;

d) alla ricostruzione della dinamica degli incidenti stradali ed eventuale accertamento di violazioni alle norme sulla circolazione stradale attraverso le immagini rilevate dagli impianti di videosorveglianza, anche del traffico urbano, qualora non siano l'unico strumento di accertamento dei fatti, ai sensi dell'art. 13 della Legge 24 novembre 1981, n. 689, rientrando dette immagini tra gli atti di accertamento idonei a ricostruire episodi, situazioni e comportamenti individuali, anche nell'ambito del procedimento sanzionatorio;

e) alla rilevazione e documentazione di violazioni al Codice della strada mediante impianti elettronici di rilevamento;

f) al controllo e alla prevenzione di situazioni di degrado caratterizzate da errati conferimenti di rifiuti e/o abbandono di rifiuti su aree pubbliche e all'accertamento sull'utilizzo abusivo di aree impiegate come discariche;

g) alla verifica sull'osservanza di ordinanze e/o regolamenti comunali al fine di adottare opportuni provvedimenti.

2. Tra le finalità di utilizzo degli impianti di videosorveglianza di cui al presente regolamento non sono comprese quelle dell'art. 4 dello Statuto dei lavoratori (legge 300 del 20 maggio 1970) relative al controllo a distanza dell'attività dei lavoratori per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

Articolo 5 – Caratteristiche tecniche

1) Per il raggiungimento delle finalità istituzionali può essere adottata ogni tecnologia di ripresa video e di captazione di immagini quali, a puro titolo esemplificativo: telecamere fisse e mobili, sistemi aeromobili a pilotaggio remoto (droni), Body-Cam (sistemi di ripresa indossabili), e Dash-Cam (telecamere a bordo veicoli di servizio), compresi selettori elettronici di veicoli muniti di targa, autovelox, telelaser, tutor, documentatori di infrazioni in area semaforica o connesse all'accesso in ZTL, nel rispetto della normativa vigente e delle caratteristiche tecniche e di sicurezza previste dal presente regolamento.
2) Le telecamere e/o i sistemi di acquisizione consentono riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.
3) Consentono altresì l'estrapolazione di filmati e di fotografie.

   Le telecamere possono essere dotate di brandeggio, di zoom ottico e digitale e possono essere dotate di infrarosso e collegate ad un centro di gestione ed archiviazione di tipo digitale.
4) In conformità alle Linee guida 3/2019 del Comitato Europeo per la protezione dei dati sul trattamento dei dati personali attraverso dispositivi video, le caratteristiche tecniche dell'impianto di videosorveglianza devono essere adeguate e improntate a garantire:

a. la sicurezza del sistema e di tutti i componenti del sistema, nonché la sua l'integrità, vale a dire protezione e controllo degli accessi in caso di interferenze volontarie e involontarie durante il funzionamento;

b. la sicurezza dei dati, quindi la riservatezza (i dati sono accessibili solo a coloro ai quali è concesso l'accesso), l'integrità (prevenzione della perdita o della manipolazione dei dati) e la disponibilità (i dati possono essere consultati ogniqualvolta sia necessario);

c. la protezione fisica delle apparecchiature di videosorveglianza da furti, atti vandalici, calamità naturali, catastrofi provocate dall'uomo e danni accidentali (ad esempio, sovratensioni elettriche, temperature estreme e riversamento di caffè). Nel caso di sistemi analogici devono essere particolarmente efficaci perché la sicurezza fisica è l'elemento più importante per la loro protezione;

5) La sicurezza del sistema e dei dati, vale a dire la protezione da interferenze volontarie e involontarie, deve comprendere:

a. protezione dell'intera infrastruttura del sistema di videosorveglianza (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni fisiche e furti;

b. protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione;

c. cifratura dei dati;

d. utilizzo di soluzioni basate su hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;

e. rilevamento di guasti di componenti, software e interconnessioni;

f. strumenti per ripristinare la disponibilità dei dati personali e l'accesso agli stessi in caso di problemi fisici o tecnici.

6) Il sistema di controllo degli accessi adottato deve essere in grado di garantire che solo le persone autorizzate possano accedere al sistema e ai dati, impedendo l'accesso agli atri; le misure che supportano il controllo fisico e logico degli accessi devono includere:

a. la garanzia che tutti i locali in cui viene effettuato il monitoraggio mediante videosorveglianza e conservate le riprese video siano protetti contro l'accesso da parte di terzi non autorizzati;

b. il posizionamento dei monitor sia effettuato in modo tale che solo gli operatori autorizzati possano visualizzarli;

c. la definizione e l'applicazione delle procedure per la concessione, la modifica e la revoca dell'accesso;

d. l'attuazione di metodi e mezzi di autenticazione e autorizzazione dell'utente, tra cui ad esempio la lunghezza delle password e la frequenza della loro modifica;

e. la registrazione e la revisione periodica delle azioni eseguite dagli utenti (con riguardo sia al sistema sia ai dati);

f. l'esecuzione del monitoraggio e l'individuazione di guasti agli accessi in modo continuativo e la risoluzione in tempi brevi delle carenze individuate.

Articolo 6 – Informativa

1) In conformità alle Linee guida 3/2019 del Comitato Europeo per la protezione dei dati e a quanto disposto degli artt. 13-14 dell'RGDP sul trattamento dei dati personali attraverso dispositivi video, è adottato un approccio scalare, attraverso una combinazione di metodi tesi ad assicurare la trasparenza, che prevede:
    a. una segnaletica di avvertimento nei pressi delle telecamere (primo livello);
    b. un'informativa di dettaglio fornita attraverso una pagina internet dove sono disponibili le informazioni di secondo livello.
2) Informativa di primo livello – segnaletica di avvertimento nei pressi delle telecamere.

Le informazioni di primo livello devono essere posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata.

Non è necessario rivelare l'ubicazione della telecamera, purché non vi siano dubbi su quali zone siano soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza.

L'interessato deve poter stimare quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.

Le informazioni fornite devono comunicare: le finalità del trattamento, l'identità del Titolare del trattamento e l'esistenza dei diritti dell'interessato, la base giuridica del trattamento e i recapiti del responsabile della protezione dei dati, la trasmissione dati a terzi, il periodo di conservazione oltre all'indicazione della pagina internet dove sono disponibili le informazioni di secondo livello.

Per la segnaletica di avvertimento è utilizzato un modello conforme al fac-simile riportato sulle Linee guida 3/2019 del Comitato Europeo per la protezione dei dati sul trattamento dei dati personali attraverso dispositivi video.

In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, dovranno essere installati più cartelli.

La segnaletica di avvertimento nei pressi delle telecamere (primo livello) nello specifico:

- dovrà essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- dovrà avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- potrà inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

3) Informativa di secondo livello – Informativa sul trattamento dei dati personali ai sensi degli artt. 13-14 dell'RGDP.

   Le informazioni di secondo livello devono essere facilmente accessibili per l'interessato e, oltre alla loro messa a disposizione attraverso la pagina internet indicata sull'informativa di primo livello, possono essere accessibili anche in formato non digitale presso gli uffici comunali. Comunque siano fornite le informazioni, queste devono contenere tutti gli elementi obbligatori a norma dell'art. 13 dell'RGPD.

4) Per l'utilizzo di particolari strumenti di acquisizione immagini e/o video di tipo mobile, l'assolvimento di fornire segnaletica di avvertimento nei pressi delle telecamere (primo livello) è assolta con l'apposizione del modello, conforme al fac-simile riportato sulle Linee guida 3/2019 del Comitato Europeo per la protezione dei dati inerenti il trattamento dei dati personali attraverso dispositivi video, sul veicolo di servizio e/o comunque prima di entrare nella zona sorvegliata, mentre l'informativa di secondo livello sul trattamento dei dati personali ai sensi degli artt. 13-14 dell'RGDP è resa disponibile attraverso la pagina internet indicata sull'informativa di primo livello.

5) Per quanto riguarda le apparecchiature tipo body-cam, l'informativa di primo livello è resa verbalmente ai presenti da parte dell'operatore all'inizio della registrazione, mentre l'informativa di secondo livello sul trattamento dei dati personali ai sensi degli artt. 13-14 dell'RGDP è resa disponibile attraverso la pagina internet indicata verbalmente.

Articolo 7 – Valutazione di Impatto sulla protezione dei dati (DPIA)

1) Ai sensi dell'art. 35, paragrafo 3, lett. c) dell'RGPD, poiché i trattamenti di dati realizzato mediante i sistemi di videosorveglianza rientrano tra le tipologie di trattamenti soggetti alla Valutazione di impatto (cd. DPIA), così come disposto dall'Autorità Garante per la protezione dei dati personali ai sensi all'art. 35, paragrafo 4 e 5, in quanto trattasi di "sorveglianza sistematica su larga scala di una zona accessibile al pubblico", l'Ente in quanto Titolare del trattamento esegue la valutazione di impatto sulla protezione dei dati personali prima della messa in esercizio degli impianti e prima di ogni successiva implementazione degli stessi.

2) Ai sensi dell'art. 35, paragrafo 2, nella valutazione di impatto il Titolare del trattamento si consulta con il responsabile della protezione dei Dati (DPO) il quale ha il compito di fornire, se richiesto, un parere in merito alla valutazione di impatto e sorvegliarne lo svolgimento.

3) Qualora la valutazione d'impatto sulla protezione dei dati, a norma dell'articolo 35 dell'RGPD, indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuarne il rischio, il Titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo (Garante protezione dei dati personali) secondo quanto previsto dall'art. 36 dell'RGPD.

Articolo 8 – Compiti e responsabilità

1) TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati è il Comune, al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.

Il Titolare del trattamento, tenuto conto della natura, del contesto e della finalità del trattamento deve garantire, ed essere in grado di dimostrare, che il trattamento è effettuato non solo in maniera conforme alla normativa ma in maniera tale da non determinare rischi e quindi di non gravare sui diritti e le libertà degli interessati.

2) RESPONSABILE "INTERNO" DEL TRATTAMENTO
(soggetto designato ai sensi dell'art. 2-quaterdecies D.Lgs. 196/2003)

Il Responsabile del Servizio di Polizia Locale è designato, ai sensi dell'Art. 2-quaterdecies D.Lgs. 196/2003, quale soggetto con specifici compiti e funzioni con il profilo di Responsabile "interno" del trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza.

Il Responsabile "interno" del trattamento è tenuto a conformare la propria azione al pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente regolamento.

Il Responsabile "interno" procede al trattamento dei dati attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

Il Responsabile "interno", se autorizzato dal Titolare ai sensi ai sensi dell'art. 2-quaterdecies D.Lgs. 196/2003, individua e nomina con propri atti i soggetti interni autorizzati al trattamento con il profilo di Incaricati/addetti del trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni dell'RGPD; detti incaricati/addetti sono opportunamente istruiti e formati da parte del Responsabile "interno" 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.

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

Il Responsabile interno è responsabile dell'accesso e della sicurezza delle centrali di controllo, degli apparati hardware e dei software.

Il Responsabile interno conserva ed è responsabile della conservazione delle chiavi e di eventuali altri disposti per l'accesso ai locali della sala di controllo, degli armadi per la conservazione degli eventuali supporti di archiviazione digitale e di ogni altro supporto informatico.

Essendo l'accesso ai dati consentito esclusivamente mediante l'inserimento della credenziale per l'autenticazione (password), per assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento di una incaricato/addetto, il Responsabile interno è il custode delle copie delle credenziali.

Le persone ammesse a qualunque titolo alle registrazioni devono essere identificate e registrate; il Responsabile interno rilascia autorizzazione per la visione dei dati registrati da parte

dell'Incaricato/addetto ed è responsabile della tenuta di un apposito Registro degli accessi (anche elettronico), nel quale sono riportati ad opera degli Incaricati/addetti almeno i seguenti dati:

- un identificativo dell'Incaricato/addetto
- la data e l'ora dell'accesso;
- i dati per i quali si è svolto l'accesso;
- la motivazione dell'accesso;

3) RESPONSABILE ESTERNO
(ai sensi dell'art. 28 dell'RGPD)

Il responsabile esterno del trattamento, ai sensi dell'art. 28 dell'RGPD, è la ditta installatrice e responsabile della manutenzione dell'impianto.

Il Titolare può nominare, qualora si rilevi la necessità, altri responsabili esterni ai sensi dell'art. 28 dell'RGPD.

I rapporti con i responsabili esterni, ai sensi dell'art. 28 dell'RGPD, sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli stati membri.

E' compito del responsabile della videosorveglianza procedere alla nomina dei responsabili ex art. 28 del RGDP.

4) INCARICATI/ADDETTI DEL TRATTAMENTO

Ai sensi dell'art. 2-quaterdecies D.Lgs. 196/2003, il Titolare e il Responsabile del Servizio Polizia municipale possono autorizzare al trattamento dei dati personali le persone che operano sotto l'autorità del Titolare nell'ambito degli Agenti di Polizia Locale.

All'Incaricato/addetto verrà affidata la custodia e la conservazione della propria password e delle chiavi della sala di controllo e dell'armadio destinato alla conservazione dei supporti magnetici. L'Incaricato/addetto del trattamento deve elaborare i dati personali ai quali ha accesso attenendosi scrupolosamente alle istruzioni del Titolare o del responsabile interno. L'Incaricato/addetto del trattamento deve trattare i dati personali ai quali ha accesso attenendosi scrupolosamente alle istruzioni del Titolare e del responsabile interno.

Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui all'art. 12 paragrafo 1, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 e a seguito di regolare autorizzazione richiesta al Responsabile interno del trattamento dei dati personali designato e previa compilazione di tutti i dati previsti dal Registro degli accessi.

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

Articolo 9 – Installazione e successive implementazioni dei sistemi di videosorveglianza

1) Per l'installazione di un impianto di videosorveglianza, sia fisso che mobile, nell'ambito del territorio del Comune è adottata la seguente procedura:

   a. Il Comando di Polizia Locale promuove la predisposizione, da parte dell'ufficio tecnico comunale preposto, del progetto che individua puntualmente tutte le componenti del nuovo sistema di videosorveglianza e le misure tecniche ed organizzative che saranno adottate per la sicurezza dei dati personali trattati. Nei casi di impianti con punti di ripresa fissa, il progetto indica in dettaglio e con precisione i punti di installazione e la zona oggetto di ripresa delle telecamere che compongono l'impianto; nel caso invece di punti di ripresa mobili indica i criteri che devono essere rispettati per individuare i punti di ripresa e le modalità con cui devono essere effettuate le riprese.

   b. La Giunta, attraverso apposita delibera, approva i siti di ripresa e/o i criteri che devono essere rispettati per individuare i punti di ripresa e le modalità con cui devono essere effettuate le riprese nel caso di punti di ripresa mobili.

   c. A seguito dell'approvazione della Giunta inerente l'individuazione dei punti e dei criteri, il Comando di Polizia Locale, dotandosi del supporto tecnico necessario e consultando il DPO, effettua la DPIA, e a seguito di una valutazione d'impatto sulla protezione dei dati, a norma dell'articolo 35 dell'RGPD, indicante che il trattamento presenta un rischio residuale basso, procede con le normali procedure adottate dal Comune all'acquisto, all'installazione ed alla messa in esercizio del nuovo impianto di videosorveglianza.

2) Per l'implementazione di impianto di videosorveglianza già in uso del Comune, è adottata la seguente procedura:

   a. Il Comando di Polizia Locale promuove la predisposizione, da parte dell'ufficio tecnico comunale preposto, del progetto che individua puntualmente tutte le modifiche necessarie alle componenti tecniche del nuovo sistema di videosorveglianza e alle misure tecniche ed organizzative adottate per la sicurezza dei dati personali trattati. Nei casi di impianti con punti di ripresa fissa, il progetto indica in dettaglio e con precisione i punti di installazione e le zone oggetto di ripresa delle telecamere che verranno eliminati, spostati o aggiunti; nel caso invece di punti di ripresa mobili indica le eventuali modifiche ed i criteri che devono essere rispettati per individuare i punti di ripresa e le modalità con cui devono essere effettuate le riprese.

   b. La Giunta, attraverso apposita delibera, approva la nuova configurazione dei siti di ripresa e/o le eventuali modifiche ai criteri che devono essere rispettati per individuare i punti di ripresa, e le modalità con cui devono essere effettuate le riprese nel caso di punti di ripresa mobili.

   c. A seguito dell'approvazione della Giunta sui punti e criteri individuati, il Comando di Polizia Locale:

      - se le modifiche sono state significative, dotandosi del supporto tecnico necessario e consultando il DPO, effettua una nuova DPIA e a seguito di una valutazione d'impatto indicante che il trattamento presenta un rischio residuale basso, procede con le normali procedure per l'acquisto, l'installazione e la messa in esercizio del nuovo impianto di videosorveglianza;

- se invece le modiche al sistema sono state di lieve entità e/o comunque tali da non compromettere la validità della DPIA precedentemente effettuata, procede direttamente con le normali procedure adottate per l'acquisto, l'installazione e la messa in esercizio del nuovo impianto di videosorveglianza.

Articolo 10 – Modalità di raccolta dei dati personali

1) I dati personali oggetto di trattamento sono trattati ai sensi dell'art. 5 dell'RGPD:
   a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
   b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 dell'RGPD, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
   c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
   d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
   e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 dell'RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
   f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2) I dati personali sono ripresi attraverso le telecamere dell'impianto di telecontrollo e di videosorveglianza e/o foto-trappole e/o altri sistemi di ripresa individuate dal Comando di Polizia Locale, installate nel territorio comunale in conformità all'elenco dei siti di ripresa, individuati e approvati con apposito atto della Giunta Comunale.
3) Presso la sala di controllo della Polizia Locale sono posizionati i monitor per la visione in diretta delle immagini riprese dalle telecamere, l'hardware e il software necessario per la visualizzazione delle registrazioni effettuate con le foto-trappole, body-cam, dash-cam e/o droni e le strumentazioni necessarie per la gestione sistema di videosorveglianza fissa.

Articolo 11 – Sicurezza dei dati

1) I dati personali oggetto di trattamento devono essere custoditi nella sala di controllo, così come i videoregistratori digitali.
2) La sala di controllo è ubicata nell'edificio della Sede Comunale, presso l'ufficio Polizia Locale. L'accesso alla sala è protetto da adeguate misure di sicurezza e da dispositivi che ne consentano l'accesso esclusivamente ai soggetti autorizzati; a tale sala possono accedere il Responsabile interno e gli incaricati. I monitor non sono comunque mai posizionati in posizioni che rendano le riprese visibili al pubblico. Il Responsabile interno è responsabile dell'accesso e della sicurezza della sala di controllo, degli apparati hardware e dei software che vi sono contenuti.
3) I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, devono essere ridotti al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
4) Devono essere adottate specifiche misure tecniche ed organizzative che consentano al Responsabile interno di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa anche attraverso la tenuta del Registro degli accessi.
5) In ogni caso, i sistemi per la videosorveglianza adottati devono garantire la registrazione dei dati relativi agli accessi (data, ora, operatore) da parte degli operatori dotati di credenziali in appositi file di log che devono essere conservati per il tempo previsto dalla legge e protetti dalla possibilità di essere manomessi.
6) Le misure di sicurezza dovranno rispettare i seguenti principi di adeguatezza e idoneità:
    a. laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
    b. per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
    c. nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti ad operazioni di manutenzione potranno accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche e solo a seguito di autorizzazione scritta del Titolare;
    d. qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del Codice penale;
    e. la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che

ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless.

Articolo 12 – Durata della conservazione dei dati

1) Le attività di videosorveglianza sono finalizzate alla tutela della sicurezza urbana, al controllo del corretto conferimento dei rifiuti solidi urbani e a prevenire l'illecito abbandono dei rifiuti, e alla luce delle recenti disposizioni normative, il termine massimo di durata della conservazione dei dati è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza.
2) L'eventuale allungamento dei tempi di conservazione per un periodo superiore ai 7 giorni deve essere valutata in base al principio di responsabilizzazione e comunque di concerto con il DPO nominato. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.
3) La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.
4) Il sistema impiegato dovrà essere programmato in modo da operare al momento prefissato 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.
5) In caso di cessazione, per qualsiasi causa, del trattamento, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento devono essere distrutti.
6) Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere formalmente che i filmati siano conservati oltre i termini di legge, 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 in questione procedere a presentare formale richiesta di acquisizione dei filmati. Tale richiesta dovrà comunque pervenire entro trenta giorni dalla data dell'evento, decorsi i quali i dati non saranno ulteriormente conservati.

Articolo 13 – Accertamenti di illeciti e indagini di Autorità Giudiziarie o di Polizia

1) Sono trattamenti distinti quelli relativi a dati personali trattati dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali e non sono soggetti all'RGPD ma alla Direttiva (UE) 2016/680 e al D.Lgs. 81/2018.
2) Il Responsabile interno o l'Incaricato/addetto può procedere alla registrazione di immagini o di spezzoni di video su supporti digitali atti a garantire adeguate misure di sicurezza (es. crittografia dei dati), nei casi in cui:

a. dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, provvedendo a darne immediata comunicazione agli organi competenti;

b. ne facciano richiesta scritta e motivata le Forze di polizia e/o l'autorità giudiziaria nello svolgimento delle proprie funzioni.

Tale registrazione deve essere corredata da una completa verbalizzazione delle operazioni svolte in modo cronologico:

a) annotazione relativa all'esecuzione del download dei filmati – Nome addetto, data e ora;

b) annotazione relativa alla visione dei filmati – nome addetto, data e ora;

c) annotazione dei fatti salienti relativi all'evento – nome addetto, data e ora;

d) annotazione relativa alle operazioni di salvataggio dei filmati e dei supporti di memorizzazione utilizzati – nome addetto, data e ora;

e) annotazione circa le eventuali estrapolazioni di fotogrammi per comporre fascicoli fotografici esplicativi per l'imitare l'accesso documentale ai filmati – nome addetto, data e ora.

3) Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di Polizia Giudiziaria e l'Autorità Giudiziaria.

Articolo 14 – Accesso ai dati

1) L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 del presente regolamento.

2) L'accesso alle immagini è consentito esclusivamente:

a. al Responsabile interno ed agli Incaricati/addetti del trattamento;

b. alle Forze di polizia e all'autorità giudiziaria, nello svolgimento delle proprie funzioni;

c. al difensore della persona sottoposta alle indagini, nell'ambito delle investigazioni difensive, a norma dell'art. 391-quater C.p.p.,

d. ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente.

e. all'interessato del trattamento (in quanto oggetto delle riprese) che presentati istanza di accesso alle immagini: l'accesso da parte dell'interessato sarà limitato alle sole immagini che lo riguardano direttamente;

f. alla società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione, nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo preventivante nominato Responsabile esterno del trattamento

ovvero, in casi del tutto eccezionali, all'amministratore informatico del sistema comunale (preventivamente individuato quale incaricato del trattamento dei dati).

L'accesso alle immagini, nei casi di cui alle precedenti lettere a) c) d) f) potrà avvenire solo ed esclusivamente inoltrando specifica richiesta motivata al Titolare del trattamento dei dati e previa corresponsione delle spese per il rilascio di copia digitale. L'accesso richiesto da organi di Polizia e di Autorità Giudiziaria è gratuito.

3) L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione generale, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre forze di polizia, deve essere oggetto di specifici accordi, in cui vengono disciplinati le modalità di accesso, gli ambiti di utilizzo e le correlate responsabilità ai sensi dell'art. 5 del decreto legge 20 febbraio 2017, n. 14 convertito con modificazioni dalla legge 18 aprile 2017, n. 48.

Articolo 15 – Diritti dell'interessato

1) I diritti che l'interessato può esercitare sono quelli previsti dagli Artt. 15, 16, 17, 18, 19, 21, 22 dell'RGDP
2) L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, la loro comunicazione in forma intelligibile e la possibilità di effettuare reclamo presso l'Autorità di controllo.
3) L'interessato ha diritto di ottenere l'indicazione:
   a. dell'origine dei dati personali;
   b. delle finalità e modalità del trattamento;
   c. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d. degli estremi identificativi del Titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2 dell'RGDP;
   e. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati/addetti.
4) L'interessato ha diritto di ottenere:
   a. l'aggiornamento, la rettifica ovvero, quando vi ha interesse, l'integrazione dei dati;
   b. 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;
   c. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
5) L'interessato ha diritto di opporsi, in tutto o in parte, per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

Articolo 16 – Il deposito dei rifiuti

1) In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'impiego di sistemi di videosorveglianza e/o foto-trappole, che per collocazione e ambito di ripresa devono essere idonei a riprendere unicamente le aree di possibile errato conferimento o illecito abbandono dei rifiuti, è consentito nel territorio comunale per il controllo del corretto conferimento dei rifiuti solidi urbani e/o per prevenire l'illecito abbandono dei rifiuti, per il perseguimento di finalità sanzionatorie in materia ambientale, ove si riveli non efficace il ricorso a strumenti e sistemi di controllo alternativi.
2) Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se 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.
3) Il trattamento dei dati personali raccolti mediante i sistemi sopra descritti dovrà essere rispettoso dei principi in materia di protezione dei dati personali così come descritti negli articoli precedenti.

Articolo 17 – Dispositivi elettronici per la rilevazione di violazioni al Codice della Strada

1) È consentito l'utilizzo di impianti elettronici per la rilevazione di violazioni al Codice della Strada, da utilizzarsi nel rispetto della normativa di riferimento.
2) I dati raccolti devono essere pertinenti e non eccedenti il perseguimento delle finalità istituzionali del titolare. È necessario limitare la dislocazione e l'angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate.
3) Più precisamente:
    a. gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;
    b. le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione 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);
    c. le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;
    d. 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 in conformità alla normativa di settore, fatte salve eventuali

esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;

e. 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;

f. in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e, pertanto, di ottenere dalla competente autorità 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.

Articolo 18 – Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

1) Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss. dell'RGPD ed alle previsioni del D.Lgs. 196/2003.

Articolo 19 – Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali

1) Chiunque subisca 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 esterno ai sensi delle disposizioni di cui all'art. 82 dell'RGPD.
2) Il Titolare o il Responsabile esterno del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
3) Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'art. 79, paragrafo 2 dell'RGPD.

Articolo 20 – Pubblicità del regolamento

1) Copia del presente regolamento sarà pubblicata all'Albo Pretorio online e potrà essere reperita sul sito internet del Comune nella sezione Amministrazione Trasparente - Atti generali.

Articolo 21 – Entrata in vigore

1) Il presente regolamento entrerà in vigore con il conseguimento della esecutività della deliberazione di approvazione, secondo le normative vigenti ed osservate le procedure dalle stesse stabilite.
2) Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.