



CITTA' DI ALESSANDRIA

REGOLAMENTO COMUNALE SULLA VIDEOSORVEGLIANZA E SUL TRATTAMENTO DEI DATI PER ATTIVITA' D'INTERESSE DELLA POLIZIA LOCALE

ADOTTATO CON DELIBERAZIONE
DELLA GIUNTA COMUNALE N. 229 DEL 26/09/2024

Sommario

Art. 1 – Premessa.....	3
Art. 2 – Principi generali	3
Art. 3 – Definizioni	5
Art. 4 – Finalità	6
Art.5 – Caratteristiche tecniche dei dispositivi utilizzati	8
Art.6 – Informativa	11
Art. 7 – Valutazione di Impatto sulla protezione dei dati.....	13
Art. 8 – Titolare e Responsabile designato al Trattamento dei dati.....	13
Art. 9 - Incaricati del Trattamento.....	15
Art. 10 - Modalità di Raccolta e di Trattamento dei Dati dei sistemi di Videosorveglianza.....	16
Art. 11 - Uso di strumenti informatici personali.....	17
Art. 12 - Utilizzo di particolari sistemi mobili	17
Art. 13- Sicurezza dei dati.....	18
Art. 14 - Accesso alle centrali di controllo	19
Art. 15 - Accesso agli impianti e ai dati.....	20
Art. 16 - Diritti dell’interessato.....	21
Art. 17 - Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale, diritto al risarcimento	22
Art. 18 – Provvedimenti attuativi	22
Art. 19 - Pubblicazione del Regolamento	23
Art. 20 - Entrata in vigore	23

Art. 1 – Premessa

1. Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali. La videosorveglianza incide sul diritto delle persone alla propria riservatezza.
2. Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti e impiegati dal Comune di Alessandria nel territorio comunale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Art. 2 – Principi generali

1. Il presente regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto di videosorveglianza cittadina ed altre tipologie di dispositivi come telecamere di lettura e riconoscimento targhe, foto trappole, body cam, dash cam, o altre apparecchiature tecnologiche che consentano il trattamento di immagini che potrebbero essere in seguito attivate nel territorio del Comune di Alessandria.
2. In particolare il presente regolamento:
 - a. definisce le modalità di utilizzo degli impianti di videosorveglianza;
 - b. disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza
3. Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto dal:
 - a. Decreto del Ministero dell'Interno 05/08/2008 (GU n.186 del 09/08/2008);
 - b. Legge n.38/2009 recante “misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori”;
 - c. Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8/4/2010 (G.U. n.99 del 29/04/2010);
 - d. Regolamento UE Generale sulla Protezione dei Dati 679/2016 GDPR, relativo “alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”;
 - e. D.P.R. n.15 del 15/01/2018 recante “Regolamento a norma dell'articolo 57 del d.lgs 196/2003, individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente a quello effettuato dalle forze dell'ordine per finalità di pubblica sicurezza.

- f. D.lgs. N.51 del 18/5/2018 “Attuazione della direttiva UE 2016/680 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”.
 - g. D.lgs n.101 del 10/08/2018 “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del Regolamento UE 679/2016 del Parlamento Europeo”.
4. La videosorveglianza in ambito Comunale si fonda sui principi applicabili al trattamento di dati personali di cui all’art. 5 GDPR e dell’art. 3 del dlgs 51/2018 e in particolare ai principi:
- a. **Principio di liceità** – Il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando è necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ossequio al disposto di cui all’art. 6, Paragrafo 1, lett. e, GDPR. La videosorveglianza comunale pertanto è consentita senza la necessità di consenso da parte degli interessati.
 - b. **Principio di necessità** – In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all’art. 5, Paragrafo 1, lett. c), GDPR, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati sono configurati per ridurre al minimo l’utilizzatore di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi o a opportune modalità che permettano di identificare l’interessato solo in caso di necessità.
 - c. **Principio di proporzionalità** – La raccolta e l’uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rivelazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un’effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione dei beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte degli addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazione agli ingressi. La proporzionalità va valutata in ogni fase del trattamento.
 - d. **Principio di finalità** – Ai sensi dell’art.5, Paragrafo 1 ,lett. b, GDPR, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. E’ consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana che il DM Interno 05/08/2008 definisce come il “bene pubblico da tutelare attraverso attività poste a difesa, nell’ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale.”

Art. 3 – 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 alla ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- b. per “**trattamento**”, qualsiasi operazione o insieme o attività, 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 “**banca dati**”, il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;
- d. per “**profilazione**”, qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l’affidabilità, il comportamento, l’ubicazione o gli spostamenti di detta persona fisica;
- e. per “**pseudonimizzazione**”, il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- f. 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 alla sua designazione possono essere stabiliti dal diritto dell’Unione o degli Stati membri;

- g. 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;
- h. per “**incaricato del trattamento**”, la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del funzionario designato al coordinamento delle attività e al controllo del trattamento;
- i. per “**interessato**”, la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
- j. 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 funzionario designato al coordinamento delle attività e al controllo del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del funzionario designato al coordinamento delle attività e al controllo;
- k. 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;
- l. 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 o consultazione;
- m. per “**diffusione**”, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- n. per “**dato anonimo**”, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
- o. Per “**GDPR**” : il regolamento UE 679/2016

Art. 4 – Finalità

1. Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza attengono allo svolgimento delle funzioni istituzionali proprie dell'amministrazione comunale in conformità a quanto previsto dal:
 - a. Legge 7 marzo 1986, n. 65, sull'ordinamento della Polizia Municipale;
 - b. D.P.R. 24 luglio 1977, n.616;
 - c. D.Lgs. 31 marzo 1998, n. 112;
 - d. D.Lgs. 18 agosto 2000, n. 267 – TUEL;
 - e. Legge 24 luglio 2008, n. 125 recante misure urgenti in materia di sicurezza pubblica;
 - f. Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana;

- g. Legge 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale;
 - h. Circolari del Ministero dell'Interno n.558/A/421.2/70/456 in data 8 febbraio 2005, n. 558/A421.2/70/195860 in data 6 agosto 2010 e n. 558/SICPART/421.2/70/224632 in data 2.3.2012;
 - i. D. Lgs. n.51/2018.
2. Nella richiamata cornice normativa e all'interno del nuovo sistema di lotta alla criminalità che attribuisce ai Comuni un ruolo strategico nel perseguire finalità di tutela della sicurezza pubblica, l'impianto di videosorveglianza del Comune di Alessandria è principalmente rivolto a garantire la sicurezza urbana che, l'art. 1 del Decreto del Ministero dell'Interno del 5 agosto del 2008, testualmente definisce come il *“bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale.”*
3. La disponibilità tempestiva di immagini presso il Comune costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale sul territorio comunale, in stretto raccordo con le Forze di Polizia. L'archivio dei dati registrati costituisce, infatti, per il tempo di conservazione stabilito per legge, un patrimonio informativo per finalità di Polizia Giudiziaria, con eventuale informativa nei confronti dell'Autorità Giudiziaria competente a procedere in caso di rilevata commissione di reati.
4. In particolare, il sistema di videosorveglianza attivato dall'Amministrazione, è finalizzato a:
- a. incrementare la sicurezza urbana e la sicurezza pubblica nonché la percezione delle stesse rilevando situazioni di pericolo e consentendo l'intervento degli operatori;
 - b. prevenire, accertare e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di “sicurezza urbana” già richiamato; le informazioni potranno essere condivise con altre Forze di Polizia competenti a procedere nei casi di commissione di reati;
 - c. tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e gli edifici pubblici e a prevenire eventuali atti di vandalismo o danneggiamento;
 - d. controllare le aree considerate a maggiore rischio per la sicurezza, l'incolumità e l'ordine pubblico;
 - e. monitoraggio del traffico;
 - f. attivare uno strumento operativo di protezione civile sul territorio comunale;
 - g. ad acquisire elementi probatori in fattispecie di violazioni amministrative o penali;
 - h. per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
 - i. monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
 - j. verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.

5. Gli impianti di videosorveglianza non potranno essere utilizzati, in base all'art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970) per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati. Gli impianti di videosorveglianza non potranno altresì essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.
6. L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.
7. La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi.
8. La possibilità di avere in tempo reale dati e immagini costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell'ambito delle proprie competenze istituzionali; attraverso tali strumenti si perseguono finalità di tutela della popolazione e del patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.
9. L'uso 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 e allo svolgimento di funzioni istituzionali di cui è investito il Comune.

Art.5 – Caratteristiche tecniche dei dispositivi utilizzati

1. Per il raggiungimento delle finalità previste nell'art.4 del suddetto regolamento rispettando i principi dell'art. 2, il Titolare del trattamento dati, o il responsabile su indicazioni del titolare, può utilizzare a seconda delle circostanze particolari dispositivi di videosorveglianza come: le telecamere fisse o mobili, telecamere di lettura e riconoscimento targhe, droni, body-cam, dash-cam, foto trappole e tutti i possibili strumenti che la tecnologia può e potrà in futuro mettere a disposizione.
2. Le telecamere fisse o mobili, posizionate nel territorio comunale sono segnalate da appositi cartelli. La loro visualizzazione, il controllo diretto per il brandeggio o gli ingrandimenti è riservato esclusivamente al personale della Polizia Locale e alle Forze dell'Ordine con essa convenzionate (attualmente Carabinieri e Polizia di Stato). L'estrazione dati delle immagini

video può avvenire solo dietro formale richiesta delle autorità competenti al Comando di Polizia Locale.

3. Le immagini trasmesse dalle telecamere sono registrate e conservate per un periodo di tempo che varia a seconda delle finalità di utilizzo in quanto, i dispositivi impiegati, a seconda della loro funzione, sono configurati con tempistiche differenti di cancellazione automatica. Le immagini acquisite dalle telecamere utilizzate per il controllo di illeciti amministrativi per il controllo del conferimento rifiuti, vengono cancellate automaticamente entro 72 ore. Oltre tale periodo verranno trattenute e conservate solo le immagini strettamente necessarie come prova indelebile della violazione per dar seguito al procedimento sanzionatorio regolato dalla legge del 24/11/1981 n° 689 e eliminate al termine dello stesso. I dati non rilevanti ai fini delle contestazioni dell'interessato saranno cancellati. Nel caso di dispositivi il cui utilizzo è destinato al controllo della prevenzione di reati e all'ordine pubblico il periodo di conservazione delle immagini è di sette giorni al termine dei quali sono cancellate con modalità automatica. La conservazione per un periodo di tempo superiore a sette giorni è ammessa esclusivamente su specifica richiesta dell'Autorità giudiziaria o della Polizia giudiziaria in relazione ad un'attività investigativa in corso.
4. I sistemi che si occupano della documentazione video-fotografica dei numeri di targa e delle informazioni relative ai dati di transito dei veicoli in infrazione, trattano immagini in cui non sono visibili le persone in transito ma solo gli autoveicoli dove in dettaglio viene riconosciuta la targa. Le immagini sono mostrate su richiesta del cittadino che ha commesso l'infrazione stradale e rimangono a corredo del procedimento amministrativo fino al termine dello stesso. I sistemi di cui sopra possono essere gestiti anche da società esterne all'Ente appositamente incaricate al trattamento di questi dati attraverso le regole previste dal GDPR e definite nel presente documento.
5. Il Corpo di Polizia Locale si potrà dotare dei seguenti sistemi:
 - a) **Droni** - Il drone è un aeromobile “guidato” da remoto: il pilota, dunque, non si trova a bordo, ma controlla il mezzo attraverso comandi che vengono trasmessi a un computer presente sul drone stesso. Questi apparecchi devono sottostare a specifiche regolamentazioni da parte di ENAC – l'Ente Nazionale per l'Aviazione Civile, che li definisce “Sistemi Aeromobili a Pilotaggio Remoto” – SAPR e sono dotati di una videocamera – fotocamera con un dispositivo elettronico di registrazione, ovvero “micro SD”, essenziale per registrare i filmati. Le immagini video, ritenute utili ai fini di polizia giudiziaria o amministrativa, devono essere salvate su supporto informatico non trascrivibile e conservate secondo le finalità descritte dal Regolamento, le altre sono sovrascritte automaticamente e, quindi, cancellate. Il trattamento dei dati è ricondotto nell'ambito del GDPR trattandosi di dati personali direttamente correlati all'esercizio dei

compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica e di polizia giudiziaria.

- b) **Dash cam** - La dash cam, dashboard camera (telecamera da cruscotto), è un dispositivo elettronico per l'acquisizione di immagini, applicabile sul parabrezza o sullo specchietto retrovisore dei veicoli di servizio in uso alla Polizia Locale che sono utilizzate al fine di registrare gli eventi che accadono all'esterno della vettura nella direzione in cui tale dispositivo è rivolto. Esse sono tutte dotate di apposita fessura per l'inserimento di un dispositivo elettronico di registrazione, ovvero "micro SD", essenziale per registrare i filmati. Questo sistema di videosorveglianza si alimenta tramite porta USB o presa accendisigari dell'auto. Le immagini video, ritenute utili ai fini di polizia giudiziaria o amministrativa, devono essere salvate su supporto informatico non trascrivibile e conservate secondo le finalità descritte dal Regolamento, le altre sono sovrascritte automaticamente e, quindi, cancellate. Le dash cam sono utilizzate nel rispetto di quanto prescritto con nota del Garante della protezione dei dati personali protocollo n. 49612 del 26 luglio 2016 il cui trattamento dei dati è ricondotto nell'ambito del GDPR trattandosi di dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica e di polizia giudiziaria.
- c) **Body cam** - Le body cam sono delle telecamere portatili, che si posizionano sulle divise degli operatori di Polizia Locale, al fine di monitorare l'attività di chi le indossa e dei soggetti con cui interagiscono. Tali micro camere sono attivabili dagli operatori durante lo svolgimento del servizio assegnato mediante pressione di un tasto posto sull'apparecchio stesso e disattivabili nella medesima modalità, ogni volta che l'operatore lo ritenga opportuno al fine di salvaguardare il proprio operato e monitorare situazioni di criticità, turbativa e illegalità, dandone preventiva comunicazione orale agli interessati. Le immagini video ritenute utili ai fini di polizia giudiziaria o amministrativa devono essere salvate su supporto informatico non trascrivibile e conservate secondo le finalità descritte nel Regolamento, le altre sono sovrascritte automaticamente e, quindi, cancellate. Le body cam sono utilizzate nel rispetto di quanto prescritto con nota del Garante della protezione dei dati personali protocollo n. 49612 del 26 luglio 2016 il cui trattamento dei dati è ricondotto nell'ambito dell'art. 53 del D.Lgs 196/2003 trattandosi di dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica e di polizia giudiziaria.
- d) **Foto trappole** - Le foto trappole (o telecamere modulari) sono sistemi di

videosorveglianza che si basano sulla rilevazione di movimento all'interno di una determinata area di ripresa, sia di giorno che di notte, grazie a led infrarossi invisibili ad occhio umano. Le immagini video sono registrate e successivamente estrapolate dal dispositivo stesso o, eventualmente, trasmesse a distanza, grazie ad una rete gsm o wi-fi. Il dispositivo si attiva grazie ad un sensore al passaggio di un corpo. Esse sono spesso utilizzate con lo scopo di contrastare l'abbandono di rifiuti o il loro errato/non autorizzato conferimento e devono essere posizionate nel territorio comunale con l'obiettivo di prevenire e/o reprimere tali azioni al fine di avviare le successive verifiche utili ad accertare eventuali violazioni amministrative e/o penali. L'attivazione del dispositivo, che è finalizzata ad attività di polizia giudiziaria e amministrativa, comporta gli obblighi d'informativa con cartelli posti prima del raggio d'azione della telecamera, secondo le prescrizioni del GDPR. L'uso di foto trappole per la prevenzione e il contrasto del fenomeno dell'abbandono incontrollato dei rifiuti, nell'espletamento di funzioni di polizia giudiziaria, è consentito nelle seguenti ipotesi:

- illecita gestione di rifiuti e loro depositi incontrollati, punibili ai sensi dell'art. 256 del D.Lgs. 152/2006;
- illecita combustione di rifiuti, punibile ai sensi dell'art. 256-bis del D.Lgs. 152/2006.

Il loro utilizzo è lecito solo se non risulta possibile, o si riveli inefficace e inattuabile, il ricorso a sistemi di controllo e monitoraggio del rispetto delle disposizioni considerando le modalità, tipologie ed orario di deposito dei rifiuti.

Le immagini video che sono ritenute utili ai fini di polizia giudiziaria o amministrativa devono essere salvate su supporto informatico non trascrivibile e conservate secondo le finalità del presente Regolamento, le altre sono sovrascritte automaticamente e, quindi, cancellate.

6. In relazione ai principi di pertinenza e di non eccedenza del GDPR, il sistema informativo ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art.6 - Informativa

1. Gli interessati devono essere sempre informati che stanno per accedere in una zona video sorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti,

manifestazioni sportive) in osservanza al regolamento UE 679/2016 GDPR e nel rispetto delle indicazioni contenute nel provvedimento del Garante della Protezione dei dati Personali 99/2010.

2. Si riporta perciò, come da esempio pubblicato sul sito del Garante, il modello di segnaletica da utilizzare. L'informativa completa sul trattamento dei dati raccolti con il sistema di videosorveglianza può essere letta nel sito internet istituzionale del Comune di Alessandria, nella sezione "Privacy" della Polizia locale.

	LA REGISTRAZIONE È EFFETTUATA DA
	CONTATTI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (se applicabile):
	LE IMMAGINI SARANNO CONSERVATE PER UN PERIODO DI
	FINALITÀ DELLA VIDEOSORVEGLIANZA
L'informativa completa sul trattamento dei dati è disponibile: <ul style="list-style-type: none">• presso i locali del titolare (reception, casse, ecc.)	È POSSIBILE ACCEDERE AI PROPRI DATI ED ESERCITARE GLI ALTRI DIRITTI RICONOSCIUTI DALLA LEGGE RIVOLGENDOSI A

L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere.

3. La segnaletica deve essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve 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.
4. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi.

5. L'Ente, nella persona del Responsabile del trattamento dei dati, si obbliga ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un anticipo di giorni dieci, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.
6. Nel caso in cui la disposizione dei cartelli informativi sia sproporzionata alle finalità del trattamento dovuto ad un controllo di una zona di ampia dimensione, si provvederà ad informare i soggetti interessati tramite apposita diffusione sul sito istituzionale della zona soggetta al trattamento.
7. Per quanto riguarda i dispositivi per il rilevamento delle infrazioni stradali è stata posizionata la cartellonistica necessaria ad avvisare l'utenza della presenza dell'impianto sempre in osservanza del provvedimento del Garante per la protezione dei dati personali in materia di videosorveglianza del 08/04/10 e dell'Art. 13 del Regolamento europeo sulla protezione dei dati personali (RGDP 2016/679).

Art. 7 – Valutazione di Impatto sulla protezione dei dati

1. In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), RGPD, qualora il trattamento di dati realizzato mediante il sistema di videosorveglianza comunale dia luogo ad una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, l'Ente procederà ad una valutazione di impatto sulla protezione dei dati personali.
2. Parimenti si procederà nei casi in cui, il trattamento di dati realizzato mediante il sistema di videosorveglianza presenti un rischio comunque elevato per i diritti e le libertà delle persone fisiche.
3. In questa fase di prima attuazione della normativa europea, l'Ente, in conformità al disposto di cui all'art. 35, Paragrafi 4 e 5, RGPD, al fine di avere maggiore chiarezza in relazione ai nuovi adempimenti, attenderà la pubblicazione obbligatoria da parte dell'Autorità Garante per la protezione dei dati personali dell'elenco delle tipologie di trattamenti soggetti alla Valutazione di impatto e l'eventuale pubblicazione dell'elenco delle tipologie di trattamenti per le quali non è richiesta una Valutazione di impatto.

Art. 8 – Titolare e Responsabile designato al Trattamento dei dati

1. Il Titolare del trattamento dei dati è il Sindaco del Comune di Alessandria, 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.

2. Il Responsabile del trattamento dei dati personali del Corpo della Polizia Locale è il Comandante (di seguito per brevità “il Responsabile”), individuato dal Titolare, designato al coordinamento delle attività e al controllo del trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza. Come da regolamento Comunale per l'attuazione del regolamento UE 679/2016 approvato dal C.C n.52/226 del 17/05/2018.
3. Il Responsabile è tenuto a conformare la propria azione al pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente Regolamento.
4. Il Responsabile 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.
5. Le competenze proprie del Responsabile sono analiticamente disciplinate nell'atto amministrativo di nomina, con il quale il Titolare provvede alla sua individuazione. In particolare:
 - a) individua e nomina con propri atti gli Incaricati del 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, GDPR; detti incaricati saranno opportunamente istruiti e formati 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;
 - b) provvede a rendere l'informativa “minima” agli interessati secondo quanto definito al precedente art. 6;
 - c) 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 GDPR 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;
 - d) assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
 - e) adotta, tenuto conto dello stato dell'arte, 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, tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del GDPR;
 - f) 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;
 - g) 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;
 - h) garantisce che il Responsabile della Protezione dei Dati (DPO) 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;

- i) 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;
- j) assicura che gli incaricati 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 attività strettamente necessarie al perseguimento delle finalità istituzionali;
- k) garantisce la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale individuato quale incaricato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del responsabile della protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;
- l) vigila sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Art. 9 - Incaricati del Trattamento

1. Il Responsabile procede ad individuare con proprio atto le persone fisiche incaricate del trattamento, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni. L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato.
2. In ogni caso, prima dell'utilizzo degli impianti, gli incaricati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.
3. Gli incaricati procedono al trattamento attenendosi alle istruzioni impartite dal funzionario designato al coordinamento delle attività e al controllo il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari. In particolare, gli incaricati devono:
 - a) 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, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
 - b) conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
 - c) mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;

- d) 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;
 - e) evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile;
 - f) mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;
 - g) conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
 - h) fornire al Responsabile ed al DPO, 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.
4. Gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del Responsabile.
5. L'utilizzo degli apparecchi di ripresa da parte degli Incaricati al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato.

Art. 10 - Modalità di Raccolta e di Trattamento dei Dati dei sistemi di Videosorveglianza

1. L'installazione delle telecamere, avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili).
2. L'attività deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.
3. Le telecamere, consentono tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.
4. 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 dell'impianto attivato. I segnali video delle unità di ripresa saranno inviati presso l'Unità di ricezione, registrazione e visione ubicata presso gli uffici della Polizia Locale. In questa sede le immagini saranno visualizzate su monitor e registrate su server dedicati.
5. I dati personali oggetto di trattamento sono:
 - a) trattati in modo lecito e secondo correttezza;
 - b) raccolti e registrati per le finalità di cui all'art. 4 del presente Regolamento e resi utilizzabili in altre attività di trattamento a condizione che si tratti di attività non incompatibili con tali scopi;
 - c) 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 ripresa video è limitata al massimo e segue le finalità previste per l'utilizzo, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.
7. Nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle richiamate 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, fatte salve specifiche esigenze di ulteriore conservazione in ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria.
8. Il sistema di videoregistrazione impiegato deve 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.
9. In caso di cessazione del trattamento, i dati personali sono distrutti.

Art. 11 - Uso di strumenti informatici personali

1. L'utilizzo di strumenti e/o dispositivi personali da parte del personale del Corpo di Polizia Locale è ammesso solo a condizione di una concreta, motivata o motivabile, immanente e specifica indisponibilità di idonea strumentazione e/o dotazione assegnata dal Comando.
2. Si ha concreta, motivata o motivabile, immanente e specifica indisponibilità di idonea strumentazione e/o dotazione assegnata laddove l'operatore non abbia in assegnazione alcun dispositivo o strumento del Comando, non possa farvi ricorso per cause tecniche, non possa far ricorso a strumenti affidati ad altri operatori e si trovi nella assoluta impossibilità di procedere ad atti del servizio o ufficio se non ricorrendo all'utilizzo di uno strumento o di un dispositivo personale.
3. È fatto obbligo di immediata cancellazione permanente dei dati personali trattati per ragioni di servizio con uno strumento o un dispositivo personale, non appena effettuato il download su sistemi in uso al Comando.

Art. 12 - Utilizzo di particolari sistemi mobili

1. Per specifiche finalità concernenti la tutela della sicurezza e ordine pubblico, la prevenzione, l'accertamento e la repressione di reati, gli operatori di Polizia Locale possono essere dotati di sistemi di microtelecamere per l'eventuale ripresa di situazioni di criticità per la sicurezza propria o altrui.

2. Le videocamere e le schede di memoria di cui sono dotati i sistemi di cui al comma precedente dovranno essere prese in carico con le modalità stabilite in un apposito disciplinare, da emanarsi. La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato. Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza delle situazioni descritte al comma 1.
3. Nel caso di assegnazione del dispositivo a singolo operatore di Polizia Locale durante lo svolgimento di servizio esterno, spetta allo stesso valutare l'attivazione del dispositivo in relazione all'evolversi degli scenari di sicurezza che facciano presupporre una criticità. Lo stesso effettuerà la disattivazione. L'operatore deve avvisare i presenti che sta effettuando una registrazione e al termine del servizio, previa compilazione di un foglio di consegna, affiderà la documentazione video realizzata all'Ufficiale di coordinamento, che provvederà a riversare le immagini su supporto di archiviazione.
4. Il trattamento dei dati personali effettuati con simili sistemi di ripresa deve rispettare i principi di cui all'art. 5, GDPR ed in particolare i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati.

Art. 13- Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del precedente art. 10.
2. I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, assicurano:
 - a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
 - b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
 - c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Ai sensi dell'art. 32, Paragrafo 2, GDPR, nel valutare l'adeguato livello di sicurezza, l'Amministrazione terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ente.
4. A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:

- a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini. Tenendo conto dello stato dell'arte ed in base alle caratteristiche dei sistemi utilizzati, i soggetti designati quali incaricati del trattamento dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le attività di competenza;
- b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà 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 immagini attività di cancellazione o di duplicazione;
- c) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 10, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;
- d) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette attività potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;
- e) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;
- f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà 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 (tecnologie Wi-Fi, Wi Max, Gprs).

Art. 14 - Accesso alle centrali di controllo

1. I dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono custoditi, ai sensi e per gli effetti dell'articolo 10, presso il datacenter e le centrali di controllo ubicate presso il Comando di Polizia Locale di Alessandria, presso la sede principale del Comune di Alessandria, nonché presso le altre sedi collegate specificate nell'art. 5 comma 2 del presente regolamento;
2. L'accesso alle centrali di controllo è consentito esclusivamente al titolare, ai responsabili e ai soggetti autorizzati, individuati ai sensi del presente regolamento.
3. L'accesso da parte di soggetti diversi da quelli indicati al comma 2 del presente articolo è subordinato al rilascio, da parte del titolare o dei responsabili, di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso.
4. L'accesso avviene in presenza di soggetti autorizzati del Comando di Polizia Locale di Alessandria individuati ai sensi del presente regolamento.
5. Fermo quanto previsto dal comma 3 del presente articolo, l'accesso alle centrali di controllo può essere consentito esclusivamente ad incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità di cui all'articolo 4 del presente

regolamento, nonché al personale addetto alla manutenzione degli impianti ed alla pulizia dei locali.

6. I responsabili impartiscono idonee istruzioni atte ad evitare assunzioni o rilevamenti di dati da parte dei soggetti autorizzati all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali garantendo la riservatezza delle informazioni.
7. Gli incaricati vigilano sul puntuale rispetto delle istruzioni impartite dai responsabili e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art. 15 - Accesso agli impianti e ai dati

1. L'accesso agli impianti di videosorveglianza di cui al presente regolamento avviene da postazioni dedicate situate all'interno della sede del Comando di Polizia Locale di Alessandria, e degli uffici di Carabinieri e Polizia di Stato di Alessandria, o di altre Forze di Polizia a ciò autorizzate, nonché da postazioni di registrazione remote qualora non sia tecnicamente possibile la trasmissione dati alla centrale operativa del Comando P.L. L'accesso ai dati può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate dal responsabile del trattamento.
2. 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.
3. L'accesso alle immagini è consentito esclusivamente:
 - a) al Titolare ed agli incaricati del trattamento;
 - b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);
 - c) 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 ovvero, in casi del tutto eccezionali, all'amministratore informatico del sistema comunale (preventivamente individuato quale incaricato del trattamento dei dati);
 - d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta al successivo art. 13. L'accesso da parte dell'interessato, sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, da parte del responsabile del servizio convenzionato di Polizia Locale o dai suoi incaricati, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle

altre persone fisiche eventualmente presenti;

- e) 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. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

Art. 16 - Diritti dell'interessato

1. In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., GDPR, su presentazione di apposita istanza, ha diritto
 - a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
 - b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
 - c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 GDPR, 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;
 - d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, GDPR.
2. L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sulla home page del sito istituzionale dell'Ente ovvero al Responsabile del servizio convenzionato di Polizia Locale in qualità di funzionario incaricato).
3. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:
 - a) il luogo, la data e la fascia oraria della possibile ripresa;
 - b) l'abbigliamento indossato al momento della possibile ripresa;
 - c) gli eventuali accessori in uso al momento della possibile ripresa;
 - d) l'eventuale presenza di accompagnatori al momento della possibile ripresa;
 - e) l'eventuale attività svolta al momento della possibile ripresa;
 - f) eventuali ulteriori elementi utili all'identificazione dell'interessato.
4. Il responsabile della protezione dei dati dell'Ente ovvero il Responsabile del servizio convenzionato di Polizia Locale accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed

il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.

5. Qualora, ai sensi dell'art. 15, paragrafo 3, GDPR, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, GDPR.
6. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
7. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.
8. Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Art. 17 - Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale, diritto al risarcimento

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, GDPR ed al Decreto Legislativo 101/2018 recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, 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”, in attuazione della delega al Governo di cui all'art. 13, L. 163/2017.
2. 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 del trattamento ai sensi delle disposizioni di cui all'art. 82, GDPR.
3. Il Titolare del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. 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'articolo 79, paragrafo 2, GDPR.

Art. 18 - Provvedimenti attuativi

1. Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi conseguenti al presente Regolamento, in particolare la predisposizione dell'elenco dei siti di ripresa, la fissazione degli orari delle registrazioni, nonché la definizione di ogni ulteriore e specifica disposizione ritenuta utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento.

Art. 19 - Pubblicazione del Regolamento

1. Copia del presente Regolamento sarà pubblicata all'albo pretorio e potrà essere reperita sul sito internet del Comune.

Art. 20 - Entrata in vigore

1. Il presente Regolamento entrerà in vigore con l'esecutività della deliberazione di approvazione, secondo le leggi vigenti.
2. Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.