COMUNE DI URZULEI

REGOLAMENTO

PER LA DISCIPLINA DEL SISTEMA DI VIDEOSORVEGLIANZA

Approvato con Deliberazione del Consiglio Comunale n. 42 del 09/10/2024

INDICE

Art. 1 – Finalità e norme di riferimento

1. Il presente regolamento disciplina le modalità di raccolta, trattamento, conservazione ed accesso dei dati personali mediante sistemi di videosorveglianza.
2. Con il presente regolamento si garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune di Urzulei 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.
3. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, ossia a distanza, mediante dei dispositivi di ripresa video, collegati ad un centro di controllo.
4. Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto dalle seguenti fonti, provvedimenti e norme tecniche:
- Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito RGPD) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Direttiva UE 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;
- DPR n. 15 del 15/01/2018 avente ad oggetto *"Regolamento a norma dell'articolo 57 del Decreto Legislativo 30 Giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia"*;
- 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);
- Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09/08/2008);
- Direttiva Ministero dell'Interno 558/SICPART/421.2/70 del 3 Febbraio 2012: *"Sistemi di videosorveglianza in ambito comunale"*;
- Legge n. 38/2009 recante *"misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori"*;
- Linee Guida 3/2019 sul trattamento di dati personali attraverso Videosorveglianza del Comitato Europeo per la Protezione dei dati adottate in data 29/01/2020;
- EN 62676-4 sistemi di videosorveglianza: linee guida di applicazione;
- EN 62676-5 sistemi di videosorveglianza: specifiche tecniche e prestazioni relative alla qualità delle immagini delle telecamere.

Art. 2 – Definizioni

Ai fini del presente Regolamento si intende:

- **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Dati personali relativi a condanne penali e reati:** dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).
- **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.
- **Banca dati:** il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e riprese video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;

- **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;
- **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;
- 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;
- **"Blocco":** la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
- **DPO** – Data Protection Officer: persona designata dal Titolare o dal Responsabile come centro di competenza per il corretto trattamento dei dati personali.
- **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratti dati personali per conto del titolare del trattamento.
- **Persone autorizzate al trattamento:** le persone fisiche autorizzate, in base a specifiche istruzioni, a compiere operazioni di trattamento dal titolare o dal responsabile.
- **Interessato:** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
- **Terzo:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.
- **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.
- **Diffusione:** il dare a conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **Dato anonimo:** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- **Strumenti elettronici:** gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
- **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.

Art. 3 – Principi generali

Ai sensi della vigente normativa in materia di sicurezza urbana i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per tutela della sicurezza urbana, la cui definizione è stata da ultimo riformulata dal d.l. 14/2017, convertito nella legge 18 aprile 2017 n. 48, all'art. 4 e definita come il bene pubblico che afferisce alla vivibilità e al decoro delle città da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio da potenziare con accordi/patti locali ispirati ad una logica di gestione consensuale ed integrata della sicurezza. Si riassumono di seguito i principi per il trattamento dei dati che saranno garantiti scrupolosamente:

• **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) RGPD. La videosorveglianza comunale pertanto è consentita senza necessità di consenso da parte degli interessati.

• **Principio di necessità:** i sistemi di videosorveglianza sono configurati per ridurre al minimo l'utilizzazione 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. Deve pertanto essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.
• **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 e il 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, abilitazione agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento. Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale dell'area effettivamente da proteggere.
• **Principio di finalità:** ai sensi dell'art. 5, paragrafo 1, lett. b) RGPD, 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 e la coesione sociale".*

Art. 4 - Base giuridica del trattamento

1. Il trattamento dei dati personali effettuati tramite il sistema di videosorveglianza può essere considerato lecito solo in quanto necessario per il perseguimento del legittimo interesse del titolare del trattamento per le finalità di cui all'art. 7, valido e prevalente sugli interessi, i diritti e le libertà dell'interessato, ai sensi dell'art. 6, comma 1, lett. f) del Reg. UE 2016/679.
2. L'interesse legittimo predetto deve avere una reale consistenza, dimostrata dal fatto che si sia verificata una situazione di disagio nella vita reale, danni o incidenti gravi in passato. Alla luce del principio di responsabilità, gli incidenti rilevanti si dovrebbero documentare, annotando in un apposito registro la data, le modalità, la perdita finanziaria e le relative accuse penali. Questi incidenti documentati possono rilevare un adeguato interesse legittimo.
3. Nel caso in cui le Forze di Polizia o l'Autorità Giudiziaria richiedano la consegna di alcuni video per lo svolgimento delle indagini, la base giuridica del trattamento deve essere rinvenuta nell'adempimento ad un obbligo di legge a cui è soggetto il Titolare del trattamento, ai sensi dell'art. 6, par. 1, lett. c), del Reg. UE 2016/679.

Art. 5 – Titolare del trattamento

1. Il Titolare del trattamento è il Comune di Urzulei, al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti autorizzati e le misure di sicurezza da adottare.
2. I designati al trattamento dei dati rilevati con apparecchi di videosorveglianza sono:
- il Responsabile della Polizia locale per le telecamere connesse alla centrale operativa;
- gli altri Responsabili dei Settori competenti per le telecamere a tutela del patrimonio comunale o non collegate alla centrale operativa della Polizia locale.
3. Il Funzionario EQ Responsabile del Settore della videosorveglianza è individuato con provvedimento dell'organo di vertice, quale persona fisica designata allo svolgimento di specifici compiti connessi al trattamento dei dati personali trattati attraverso il sistema di videosorveglianza, ivi comprese le collegate

funzioni di vigilanza e controllo, in conformità alle previsioni di cui all'art. 2-*quaterdecies*, comma 1, del D.Lgs. n. 196/2003.
I compiti e le funzioni specifiche attribuite al Funzionario EQ espressamente designato al trattamento dei dati personali effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune, sono analiticamente disciplinati nel Decreto con il quale il Titolare provvede alla sua designazione.
4. Gli specifici compiti e le funzioni connesse al trattamento dei dati personali attribuiti al Funzionario EQ assegnatario dell'esercizio della videosorveglianza sono quelle di seguito indicate:
a) individuare nominativamente ed autorizzare al trattamento dei dati le persone che nell'ambito del Settore di competenza siano preposte ad attività di trattamento sotto l'autorità diretta del titolare, a ciò provvedendo con propria determinazione, impartendo loro apposite istruzioni organizzative ed operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29 RGPD e art. 2-*quaterdecies*, comma 2, D.Lgs. 196/03;
b) garantire che dette persone autorizzate siano opportunamente istruite e formate al trattamento con riferimento alla tutela del diritto protezione dei dati 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, in conformità alle previsioni di cui agli artt. 29 e 32, paragrafo 4 del RGPD;
c) impartire alle persone autorizzate al trattamento apposite istruzioni organizzative e operative affinché il trattamento di dati operato mediante i sistemi di videosorveglianza sia realizzato nel rispetto dei principi di cui all'art. 5 del RGPD e ciò al fine di assicurare, in particolare, che i dati siano acquisiti e trattati esclusivamente per le finalità connesse all'esercizio dei sistemi di videosorveglianza in quanto determinate, esplicite e legittime;
d) rendere l'informativa "minima" agli interessati, in conformità alle specifiche tecnico operative del sistema di videosorveglianza;
e) assicurare che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
f) tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adottare tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del RGPD;
g) assistere il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;
h) assistere il Titolare nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 32 del RGPD e coadiuvarlo nella concreta adozione di misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;
i) garantire l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, formalizzare tempestivamente la proposta di adozione delle misure necessarie nei confronti dell'Ente;
j) assistere il Titolare nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato, ai sensi degli artt. 33 e 34 del RGPD;
k) assistere il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD;
l) affiancare il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del RGPD, nell'istituzione e aggiornamento del Registro delle attività dei trattamento, tenuto in forma scritta, anche in formato elettronico;
m) fornire al Responsabile per la Protezione dei Dati, ogni elemento, dato e informazione necessari alla regolare formazione, tenuta e all'aggiornamento del Registro delle attività dei trattamenti di cui all'art. 30, paragrafo 1, RGPD;
n) garantire che il Responsabile della Protezione dei Dati designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;

o) custodire e controllare i 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;
p) assicurare che gli autorizzati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantire che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
q) garantire 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;
r) vigilare sul rispetto da parte degli autorizzati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Art. 6 – Persone autorizzate al trattamento

1. Le persone fisiche autorizzate al trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni, sono individuate con provvedimento determinativo del Funzionario EQ Responsabile di Settore, ai sensi dell'art. 2-quaterdecies, comma 2, del D.Lgs. 196/03 e ss.mm.ii.
2. 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.
3. Le persone autorizzate procedono al trattamento attenendosi alle disposizioni ed alle illustrazioni impartite dal Funzionario EQ Responsabile di Settore il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari. In particolare, le persone autorizzate devono:

- per l'accesso alle banche dati informatiche, utilizzate 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;
- 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;
- mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
- 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;
- evitare di creare banche dati nuove senza autorizzazione espressa dal Funzionario EQ Responsabile di Settore al trattamento dei dati;
- conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
- fornire al Funzionario EQ Responsabile di Settore ed al Responsabile della Protezione dei dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

4. Tra i soggetti designati quali autorizzati verranno individuati, con l'atto di nomina, le persone cui è affidata la custodia e la conservazione delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti magnetici.
5. Le persone autorizzate al trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del Funzionario EQ Responsabile di Settore.
6. L'utilizzo degli apparecchi di ripresa da parte delle persone autorizzate al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento.

Art. 7 – Informativa

1. Ai sensi dell'art. 13 del Reg. UE 2016/679, il titolare del trattamento deve fornire agli interessati dettagliate informazioni in merito al trattamento dei dati effettuato. Alla luce del volume di informazioni che

è necessario fornire all'interessato, è preferibile seguire un approccio a più livelli: le informazioni più importanti dovrebbero essere visualizzate sul cartello di avvertimento stesso (primo livello o informativa semplificata) mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).
2. Le informazioni sul sistema di videosorveglianza possono essere fornite in combinazione con un'icona al fine di fornire, in modo facilmente visibile, comprensibile e chiaramente leggibile, una panoramica significativa del trattamento previsto.
3. Il Comune di Urzulei, nelle strade e nelle piazze in cui sono posizionate le telecamere, affigge una adeguata segnaletica su cui deve essere riportata la seguente dicitura: *"Comune di Urzulei – Area video sorvegliata. La registrazione è effettuata dal Comune per fini di prevenzione, sicurezza e viabilità (art. 13 del Codice in materia di protezione dei dati personali – D.Lgs. n. 196/2003"* .
4. L'interessato deve essere in grado di stimare quale area è acquisita da una telecamera in modo da poter evitare la sorveglianza o adattare il suo comportamento, se necessario.
5. I cartelli affissi dovrebbero trasmettere le informazioni più importanti, come:
a) i dettagli delle finalità del trattamento;
b) l'identità del Titolare del trattamento;
c) l'esistenza dei diritti dell'interessato;
d) le informazioni sui maggiori impatti del trattamento come, ad esempio, gli interessi legittimi perseguiti dal Titolare del trattamento (o da una terza parte) e i dettagli di contatto del Titolare della Protezione dei Dati;
e) le informazioni più dettagliate di secondo livello, dove e come trovarle;
f) tutte le informazioni che potrebbero impressionare l'interessato, come la trasmissione dei dati a terzi, in particolare se si trovano al di fuori dell'UE, o il relativo periodo di conservazione. Se queste informazioni non sono indicate, l'interessato dovrebbe presumere che esiste solo un monitoraggio in tempo reale (senza alcuna registrazione o trasmissione di dati a terzi);
g) dove trovare le ulteriori informazioni sul trattamento dei dati, disponibili in un luogo facilmente accessibile all'interessato tramite fonte digitale (ad esempio QR-code o indirizzo di un sito Web) o analogica (es. banco informazioni).
6. L'informativa completa deve contenere tutti i dati previsi dall'art. 13 del Reg. UE 2016/679 e deve essere messa a disposizione degli interessati con modalità di facile accesso.
7. Tenuto conto del fatto che le riprese potrebbero, seppur in via esclusivamente accidentale, riguardare i dipendenti e collaboratori, il titolare deve mettere a disposizione del personale una copia del presente regolamento e una copia dell'informativa sul trattamento dei propri dati personali, consultabili in qualunque momento anche mediante estrazione di copia.
8. Sul sito istituzionale del comune e presso gli uffici individuati è disponibile l'informativa concernente le finalità degli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso dell'interessato secondo quanto previsto dal GDPR relativamente alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla direttiva polizia relativamente 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.

Art. 8 – Finalità dei sistemi e architettura degli impianti

1. Le finalità del suddetto impianto, del tutto conformi alle funzioni istituzionali demandate al Comune, sono:
- prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e, quindi, assicurare maggiore sicurezza ai cittadini;
- tutelare gli immobili di proprietà dell'Amministrazione Comunale e prevenire eventuali atti di vandalismo o danneggiamento del patrimonio pubblico;
- rilevare situazioni di pericolo per la sicurezza pubblica, consentendo l'intervento degli operatori;
- controllare i flussi di traffico e viabilità.
2. Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato ai fini di:
- attuazione di un sistema di sicurezza integrata ai sensi dell'art. 2 del dl 14/2017;
- tutela della sicurezza urbana e della sicurezza pubblica;
- tutela degli operatori e del patrimonio comunale;
- tutela della protezione civile e della sanità pubblica;
- tutela della sicurezza stradale;

- tutela ambientale e polizia amministrativa;
- prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali
- arresto in flagranza differito (Art. 10 co. 6 quater D.L. 14/2017)
- attuazione di atti amministrativi generali (art. 2-ter Codice privacy novellato dalla legge 205/2021 e art. 5 D. lgs 51/2018).

3. Il sistema di videosorveglianza implica il trattamento di dati personali che possono essere rilevati da telecamere tradizionali eventualmente munite di algoritmi di analisi video, metadatazione, conteggio delle persone e verifica dei comportamenti o varchi lettura targhe connessi a black list o altre banche dati, in grado di verificare la regolarità di un transito di un veicolo.
4. Il comune promuove, per quanto di propria competenza, il coinvolgimento dei privati per la realizzazione di singoli impianti di videosorveglianza, orientati comunque su aree o strade pubbliche o ad uso pubblico, nel rispetto dei principi di cui al presente regolamento, previa valutazione di idoneità dei siti e dei dispositivi, normalmente senza connessioni al sistema centrale e senza possibilità di accesso ai filmati, ma con connessioni preferibilmente stand alone. I privati interessati assumono su di sé ogni onere per acquistare le attrezzature e renderle operative in conformità alle caratteristiche tecniche dell'impianto pubblico, le mettono a disposizione dell'ente a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa. Il comune può assumere su di sé gli oneri per la manutenzione periodica e la responsabilità della gestione dei dati raccolti.
5. Nei casi di cui al comma precedente, in accordo con il comune e previa stipula di apposita convenzione, i soggetti privati che hanno ceduto i propri impianti di videosorveglianza all'ente possono decidere, con oneri a proprio carico, di affidare il controllo in tempo reale delle immagini ad un istituto di vigilanza privato, con il compito di allertare ed interessare in tempo reale le forze di polizia in caso di situazioni anomale.
6. Nel rispetto delle finalità previste nel presente regolamento, dalle immagini di videosorveglianza potranno essere acquisiti elementi utili alla verbalizzazione di violazioni amministrative, nel rispetto delle vigenti normative e regolamenti.

Art. 9 – Trattamento e conservazione dei dati

1. I dati personali oggetto di trattamento effettuato con strumenti elettronici nel rispetto delle misure minime indicate dalla normativa relative alla protezione delle persone fisiche sono:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per le finalità di cui al precedente articolo e resi utilizzabili per operazioni compatibili con tali scopi;
c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
d) conservati per le telecamere collegate alla centrale operativa per un periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione. Tale termine potrà essere esteso per finalità di indagine, mediante un ulteriore atto in applicazione della Legge 205/2021. Di tale ulteriore conservazione se ne darà notizia nell'informativa completa ai sensi dell'art. 13 del Reg. UE 2016/679;
e) conservati per le telecamere a tutela del solo patrimonio comunale (o per altre telecamere non collegate alla centrale operativa del corpo) per un periodo non superiore a 72 ore successive alla rilevazione, fatte salve speciali esigenze di sicurezza urbana e sicurezza pubblica.
2. I dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza. Il posizionamento delle telecamere è espressamente individuato con atto della Giunta Comunale su progetto predisposto dal Responsabile della Settore Tecnico e successivamente potrà essere eventualmente ampliato, secondo gli sviluppi futuri del sistema, mediante approvazione di apposite deliberazioni sempre ad opera della Giunta Comunale.
3. Le telecamere di cui al comma 2 consentono, tecnicamente, riprese video diurne/notturne 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 delle riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa saranno raccolti da una stazione di monitoraggio e controllo ubicata presso la centrale operativa del Servizio di Polizia Locale. In questa sede le immagini saranno registrate su supporto magnetico da un sistema appositamente predisposto e visualizzate su monitor. L'impiego del sistema di videoregistrazione si rende necessario per ricostruire le varie fasi dell'evento, nell'ambito delle finalità previste all'articolo 8, comma 1, del presente Regolamento. Le telecamere devono presentare le

caratteristiche descritte in un'apposta relazione rilasciata dalle ditte installatrici, e tale materiale va conservato agli atti dal Titolare.
5. In relazione alle capacità di immagazzinamento dei dati forniti tramite i videoregistratori digitali, in condizioni di normale funzionamento le immagini riprese in tempo reale distruggono quelle già registrate in un tempo inferiore a quello citato, in piena osservanza della normativa vigente sulla privacy.

Art. 10 – Modalità di raccolta dei dati

1. 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 alla 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.
2. Ai sensi dell'art. 32, paragrafo 2, RGPD, 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.
3. 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 autorizzati al trattamento dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare unicamente le operazioni 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 operazioni di cancellazione o di duplicazione;
c) 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 operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche, che 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.

Art. 11 - Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto, compatibilmente con i fini investigativi a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati ex art. D.lgs 51/2018:
a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;
b) di essere informato sugli estremi identificativi del titolare e del designato al trattamento, oltre che 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 ed in generale di tutto quanto previsto ex art. 13 GDPR e art. 10 e ss. D. lgs 51/2018;
c) di ottenere:

- la conferma dell'esistenza o meno di dati personali che lo riguardano;
- la trasmissione in forma intelligibile dei medesimi dati e della loro origine;
- la cancellazione nei casi previsti dal Regolamento UE 2016/679 qualora sussista uno dei motivi di cui all'art. 17 del 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, nei casi previsti dal Regolamento UE 2016/679, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi 9 dell'art. 21 del GDPR. Il designato informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti.

e) di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle ipotesi specificate all'art. 18 del GDPR. In tali casi i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico.

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

3. L'istanza per l'esercizio dei diritti dell'interessato è presentata alternativamente al Titolare del Trattamento o al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP.

4. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:
- il luogo, la data e la fascia oraria della possibile ripresa;
- l'abbigliamento indossato al momento della possibile ripresa;
- gli eventuali accessori in uso al momento della possibile ripresa;
- l'eventuale presenza di accompagnatori al momento della possibile ripresa;
- l'eventuale attività svolta al momento della possibile ripresa;
- eventuali ulteriori elementi utili all'identificazione dell'interessato.

Il Funzionario EQ del Settore in cui è incardinato il servizio di videosorveglianza 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 l'interessato chieda, ai sensi dell'art. 15, paragrafo 3, RGPD, 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, ai sensi dell'art. 15, paragrafo 4, RGPD.

6. Nel caso di esito negativo all'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. 12 – 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 al presente Regolamento.

2. L'accesso alle immagini è consentito esclusivamente:

a) al Funzionario EQ del Settore in cui è incardinato il servizio di videosorveglianza ed alle persone autorizzate al 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 che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta all'art. 11 del presente Regolamento. 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, in conformità alle istruzioni

impartite dal Funzionario EQ, una schermatura/sfocatura 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 eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

Art. 13 - Responsabili esterni del trattamento

Nel caso in cui l'installazione e la successiva gestione del sistema di videosorveglianza vengano effettuati da una società esterna, quest'ultima deve essere preliminarmente nominata Responsabile esterno del trattamento ai sensi dell'art. 28 del Reg. UE 2016/679, in relazione all'ambito di trattamento definito. La predetta nomina, con valenza contrattuale, deve essere redatta in forma scritta e deve contenere le istruzioni in merito al corretto trattamento dei dati personali. A seguito della sua sottoscrizione, il responsabile è tenuto al rispetto di tutti gli obblighi dettati dall'art. 28 del Reg. UE 2016/679, tra i quali mettere a disposizione del Titolare del trattamento le informazioni necessarie per dimostrare il rispetto degli obblighi normativi e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento.

Art. 14 - Misure di sicurezza tecniche

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo 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. La sicurezza del sistema e dei dati, ovvero la protezione da interferenze intenzionali e non intenzionali durante la normale attività dovrebbe includere:
a. protezione dell'intera infrastruttura di videosorveglianza (comprese telecamere remote, cavi e alimentatore) contro manomissioni fisiche e furti;
b. protezione della trasmissione di filmati con canali di comunicazione sicuri contro l'intercettazione;
c. crittografia dei dati;
d. utilizzo di soluzioni basate su hardware e software come firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;
e. rilevamento di guasti di componenti, software e interconnessioni;
f. mezzi per ripristinare la disponibilità e l'accesso al sistema in caso di incidente fisico o tecnico. In base alle caratteristiche dei sistemi utilizzati, i soggetti autorizzati al trattamento o, eventualmente, responsabili esterni del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza.
Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (controllo dei log). Il controllo degli accessi garantisce infatti che solo le persone autorizzate possano accedere al sistema e ai dati, mentre viene impedito agli altri di farlo. Le misure che supportano il controllo dell'accesso fisico e logico devono:
a. garantire che tutti i locali in cui viene effettuato il monitoraggio della videosorveglianza e vengono archiviate le riprese video siano protetti contro l'accesso non controllato da parte di terzi;
b. definire ed applicare le procedure per la concessione, la modifica e la revoca dell'accesso fisico e logico;
c. implementare metodi e mezzi di autenticazione e autorizzazione dell'utente, incluso ad esempio la lunghezza delle password e la frequenza di modifica;
d. registrare e rivedere periodicamente le azioni eseguite dall'utente (sia sul sistema che sui dati) tramite il controllo dei log di accesso;
e. effettuare il monitoraggio e il rilevamento degli errori di accesso in modo continuo e affrontare tempestivamente le carenze.
Nel caso in cui il sistema sia configurato 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.

Nel caso in cui sia necessario effettuare interventi di manutenzione, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini.

Art. 15 - DPIA (Data Protection Impact Assessment)

Ai sensi dell'articolo 35, paragrafo 1, Il Titolare è tenuto ad effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) quando un tipo di trattamento dei dati può comportare un rischio elevato per i diritti e la libertà delle persone fisiche e se il trattamento costituisce un monitoraggio sistematico di un'area accessibile al pubblico su larga scala. Nello specifico, secondo il chiarimento interpretativo fornito dal Garante per la protezione dei dati personali con l'Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979 - Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018 contenente l'Elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto] la valutazione d'impatto è obbligatoria quando *"dai trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8)."* .
Il Titolare del trattamento dei dati dovrebbe quindi effettuare tale valutazione e, sulla base del risultato della DPIA eseguita, dovrebbe determinare la scelta delle misure di protezione dei dati da implementare. È anche importante notare che se i risultati della DPIA indicano che il trattamento comporta rischi elevati nonostante le misure di sicurezza pianificate dal Titolare del trattamento, sarà necessario prima di iniziare il trattamento consultare l'Autorità di controllo competente.

Art. 16 - Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti, ceduti o conservati secondo quanto previsto dal GDPR relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, 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.
2. A seguito di ciò i dati raccolti dovranno essere distrutti o conservati per fini esclusivamente istituzionali.
3. La temporanea sospensione dell'attività di videosorveglianza a causa di interventi manutentivi o malfunzionamento, non necessita di notificazione al Garante, ma verrà annotata dal Responsabile e comunicata al Titolare del trattamento dati.

Art. 17 – Mezzi di ricorso, tutela amministrativa e giurisdizionale

Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa e giurisdizionale, si rinvia integralmente a quanto previsto dagli artt. 77 e ss., RGPD ed alle previsioni che saranno contenute nel Decreto Legislativo di prossima emanazione 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.

Art. 18 – Provvedimenti attuativi

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 – Norma di rinvio

Per quanto non disciplinato dal presente Regolamento si rinvia al D.lgs 51/2018 e al D.lgs 101/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Art. 20 – Modifiche regolamentari

I contenuti del presente Regolamento dovranno essere aggiornati nei casi di variazioni delle normative in materia di trattamento dei dati personali, gerarchicamente superiori.

Art. 21 – Pubblicità ed entrata in vigore del Regolamento

1. Copia del presente Regolamento sarà tenuta a disposizione del pubblico perché ne possa prendere visione in qualsiasi momento.
2. Copia dello stesso sarà pubblicata per quindici giorni all'Albo pretorio on line dell'Ente e all'apposita sezione del sito internet del Comune "Statuto e Regolamenti" ed entrerà in vigore il giorno successivo all'ultima pubblicazione.