

REGOLAMENTO PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA SUL TERRITORIO DELLA COMUNITA' RIVIERA FRIULANA

Approvato con Deliberazione dell'Assemblea n. 2 del 03.02.2026

Sommario

1. Articolo 1 - Oggetto	3
2. Articolo 2 - Definizioni	3
3. Articolo 3 – Finalità e principi del trattamento del Sistema di videosorveglianza	5
4. Articolo 4 – Caratteristiche tecniche del sistema di videosorveglianza	7
5. Articolo 5 Accordo di contitolarità dei dati	7
6. Articolo 6 – Condivisione e accesso al Sistema di videosorveglianza da parte di soggetti terzi ..	7
7. Articolo 7 – Titolarità del trattamento dei dati personali nei sistemi di videosorveglianza	8
8. Articolo 8 – Valutazione d’impatto sulla protezione dei dati personali e consultazione preventiva con l’Autorità di Controllo	8
9. Articolo 9 – Referente interno del sistema di videosorveglianza.....	8
10. Articolo 10 – Amministratore di sistema del sistema di videosorveglianza	8
11. Articolo 11 - Registro delle attività di trattamento	9
12. Articolo 12 – Gestione violazione della sicurezza - data breach.....	10
13. Articolo 13 - Personale autorizzato al trattamento e persone autorizzate ad accedere ai locali	10
14. Articolo 14 - Persone autorizzate ad accedere ai dispositivi di ripresa installati sul territorio	11
15. Articolo 15 - Nomina a responsabile ai sensi dell’art. 28 Reg. Eu. 679/2016 per interventi tecnici sul sistema di videosorveglianza.....	11
16. Articolo 16 – Individuazione luoghi di ripresa e conservazione dati	11
17. Articolo 17 - Prescrizioni da adottare per i dati trattati	11
18. Articolo 18 - Informazioni rese al momento della raccolta	12
19. Articolo 19 – Accesso alle immagini del sistema di videosorveglianza	12
20. Articolo 20 - Comunicazioni	12
21. Articolo 21 – Trattamento per finalità di polizia giudiziaria	13
22. Articolo 22 - Pubblicità del regolamento.....	13
23. Articolo 23 – Sopravvenienza di nuove disposizioni normative	13
24. ALLEGATO A – Individuazione dei punti di ripresa	13

1. Articolo 1 - Oggetto

1. Il presente regolamento disciplina il trattamento dei dati personali, effettuato mediante il sistema di videosorveglianza installato sul territorio di competenza della Comunità Riviera Friulana (di seguito "Ente").
2. Per tutto quanto non disciplinato nel presente regolamento, si rinvia a quanto disposto dal:
 - 2.1. **Regolamento UE n. 679/2016** del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
 - 2.2. **D.lgs. 30 giugno 2003 n. 196**: "*Codice in materia di protezione dei dati personali*" e successive modifiche ed integrazioni (s.m.i.);
 - 2.3. **D.lgs. del 18 maggio 2018, n. 51**, recante: "*Attuazione della direttiva (UE) 2016/680 del Parlamento e del consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, nonché alla libera circolazione dei tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*";
 - 2.4. **Decreto del Presidente della Repubblica n. 15 del 15.01.2018**, recante "*Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia*";
 - 2.5. **Direttiva UE n. 2016/680** del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
 - 2.6. **Art. 54 del D.lgs. 18 agosto 2000 n. 267** e successive modificazioni;
 - 2.7. **Circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/N471**;
 - 2.8. **D.Lg. 23 febbraio 2009 n. 11, coordinato con Legge di conversione n. 38 del 23 aprile 2009** recante: "*Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*", ed in particolare dall'art. 6;
 - 2.9. "**Provvedimento in materia di videosorveglianza**" emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010;
 - 2.10. **Circolare del Ministero dell'Interno del'2 marzo 2012, n. 558/SICPART/421.2/70/224632**; *avente per oggetto: Sistemi di videosorveglianza in ambito comunale – Direttiva che indica nel Comitato provinciale per l'ordine e la sicurezza pubblica come una "stabile modalità di valutazione degli apparati di videosorveglianza in ambito comunale" linea condivisa dall'ANCI.*
 - 2.11. **Decreto-legge 20 febbraio 2017, n. 14**, Disposizioni urgenti in materia di sicurezza delle città convertito con L. 18 aprile 2017, n. 48.

2. Articolo 2 - Definizioni

Ai fini del presente regolamento si intende:

- per "**trattamento**", qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- per "**dato personale**", ai sensi dell' art. 4 n.1 Reg. EU 679/2016, 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;
- per "**dati identificativi**", i dati personali e le informazioni che permettono l'identificazione diretta dell'interessato;
- per "**dati particolari**", ai sensi dell'art. 9 Reg. EU 679/2016, i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché quelli genetici, dati biometrici (intesi a identificare in modo univoco una persona fisica), dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- per "**dati giudiziari**", dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione;
- 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;
- per "**Referente interno del sistema di videosorveglianza**", la persona fisica che sovrintende l'attività di videosorveglianza nominata con apposito atto del Titolare del trattamento;
- per "**incaricati o autorizzati del trattamento**", le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal Referente interno del servizio di videosorveglianza;
- per "**interessato**", la persona fisica cui si riferiscono i dati personali;
- per "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal responsabile, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies D.lgs. 196/2003 così come modificato dal D.lgs. 101/2018, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- per "**diffusione**", il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per "**dato anonimizzato**", il dato che non può essere associato ad un interessato identificato o identificabile;
- per "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
- per "**dati biometrici**", ai sensi dell'art. 4 n.14 Reg. EU 679/2016, il dato personale, ottenuto da un trattamento tecnico specifico, relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consente o ne conferma l'identificazione univoca, quale l'immagine facciale o i dati dattiloscopici;
- per "**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- per "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica, anche indiretta, dell'identità;
- per "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- per "**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- per "**sistema di autorizzazione**", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
- per "**videocamere**", i dispositivi di ripresa video installati sul territorio comunale e che costituiscono il sistema di videosorveglianza oggetto del presente regolamento;
- per "**Body Cam**", telecamere portatili, indossabili, che si posizionano in genere sulla testa o su una spalla, al fine di garantire la sicurezza degli agenti che effettuano interventi;

- per “**Dash Cam**”, piccole videocamere che vengono posizionate sulle autovetture, generalmente sul cruscotto, e in grado di registrare quello che accade all’esterno dell’abitacolo;
- per “**Drone**”, aeromobile a pilotaggio remoto ossia un apparecchio volante caratterizzato dall'assenza del pilota a bordo. Il suo volo è controllato dal computer a bordo del mezzo aereo oppure tramite il controllo remoto di un navigatore o pilota, sul terreno o in altre posizioni;
- per “**fototrappole**”, sistemi in grado di riprendere in modo del tutto automatico un corpo che entra nel raggio di azione di apposito sensore e viene inquadrato dal dispositivo, senza il bisogno della presenza fisica dell'operatore;
- per “**sistema di videosorveglianza**”, l’insieme dei dispositivi di ripresa, costituiti dalle videocamere, dalle Body Cam e Dash Cam, dai droni e delle Fototrappole, dai dispositivi di rilevamento targhe installati o altra strumentazione di rilevazione di immagini attivi sul territorio della Comunità;
- per data breach o «violazione dei dati personali» si intende qualsiasi violazione della sicurezza che porti, accidentalmente o illecitamente, alla distruzione, perdita, alterazione, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o altrimenti trattati nell’ambito del sistema di videosorveglianza. (cfr. art. 4 n.12 GDPR).

3. Articolo 3 – Finalità e principi del trattamento del Sistema di videosorveglianza

1. Il presente regolamento garantisce che il trattamento dei dati personali effettuato mediante il sistema di videosorveglianza nel territorio della Comunità Riviera Friulana si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Le disposizioni del presente regolamento, le figure dallo stesso contemplate, gli obblighi a carico dei soggetti ivi previsti, rappresentano un modello di procedura standardizzata.
2. Per il trattamento dei dati disciplinato dal presente regolamento devono essere rispettate le disposizioni ed i principi del Reg. Eu 679/2016, del D.lgs. 30 giugno 2003 n. 196 (così come modificato dal D.lgs. 101/2018) nonché tutte le vigenti norme dell’ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell’immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela, oltreché le norme in tema di tutela dei lavoratori, con particolare riferimento all’art. 4 della legge 300/1970 (Statuto dei lavoratori) e le norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni.
3. Monitor per la visione in diretta delle immagini riprese dalle telecamere e relativi server di gestione devono essere installati in luoghi sicuri e protetti dalla vista di soggetti non autorizzati o da accessi abusivi.
4. I dispositivi di ripresa e le soluzioni software che trattano dati particolari o che si basano sull’intelligenza artificiale, possono essere utilizzati nel rispetto della normativa vigente e previa positiva valutazione d’impatto ai sensi dell’art. 35 del Reg. Eu 679/2016.
5. Il sistema di videosorveglianza potrà essere utilizzato dalla Comunità Riviera Friulana, come previsto dall’art. 2 ter del D.lgs 196/03, per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri, quando necessario o utile al perseguimento delle seguenti finalità di trattamento:

5.1. sicurezza e prevenzione:

- 5.1.1. Protezione e incolumità degli individui (profili di sicurezza urbana di competenza dell’Ente);
- 5.1.2. Ordine e sicurezza pubblica (anche mediante collegamento e utilizzo del sistema di videosorveglianza da parte di Forze di Polizia esterne);
- 5.1.3. Prevenzione, accertamento e repressione dei reati (anche mediante collegamento e utilizzo sistema di videosorveglianza da parte di Forze di Polizia esterne);
- 5.1.4. Raccolta di elementi utili all'accertamento ed alla repressione dei comportamenti illeciti;
- 5.1.5. Razionalizzazione e miglioramento dei servizi al pubblico;

- 5.1.6. Rilevazione, prevenzione e controllo delle infrazioni accertate dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla Legge;
- 5.1.7. Tutela di coloro che più necessitano di attenzione: minori e anziani, portatori di handicap;
- 5.1.8. Monitoraggio del traffico;
- 5.1.9. Controllo di determinate aree ai fini della tutela ambientale;
- 5.1.10. Prevenzione, accertamento e repressione degli illeciti nonché emissione di sanzioni amministrative derivanti dal mancato rispetto della normativa, nazionale e comunale, concernente lo smaltimento dei rifiuti.

5.2. Tutela del patrimonio:

- 5.2.1. Tutela dei beni di proprietà o in gestione all'Ente. Nello specifico il sistema di videosorveglianza può essere utilizzato per tutela del patrimonio pubblico e privato, per la prevenzione ed accertamento di eventuali atti di vandalismo o danneggiamento;

5.3. Codice della strada:

Le immagini potranno essere utilizzate al fine della contestazione automatizzata da remoto di sanzioni amministrative per violazioni del Codice della Strada e altre norme quando ciò è previsto dalla legge. Le immagini potranno altresì essere utilizzate per l'esercizio dei poteri e contestazioni dirette effettuate dal personale qualificato appartenente alle Forze di Polizia Statale e/o locale. Resta salva la possibilità per l'Ente di compiere accertamenti relativi alle violazioni al Codice della Strada con dispositivi omologati, a ciò dedicati, che potranno in ogni caso essere segnalati da apposita cartellonistica. Tali strumenti utilizzati dovranno riprendere solo la targa del veicolo e gli altri elementi necessari per la predisposizione del verbale di accertamento delle violazioni (ad esempio la tipologia di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta). Le fotografie e le riprese video non possono essere inviate al domicilio dell'interessato. A tale soggetto potranno essere inviate indicazioni che gli consentano di richiedere la visione delle immagini e che comunque potranno essere visionate anche presso gli uffici competenti con le modalità indicate dall'Amministrazione; in tal caso, dovranno comunque essere oscurati o resi non riconoscibili i passeggeri ed i terzi non direttamente coinvolti nella guida ed eventualmente presenti nel veicolo.

- 5.4. **Supporto al sistema di protezione civile nel territorio e monitoraggio** delle aree eventualmente a rischio gestite dalla Comunità Riviera Friulana.

- 6. Tutte le attività e trattamenti svolte in applicazione del presente regolamento devono conformarsi ai seguenti principi:

Principio di necessità: non sono e non dovranno essere utilizzati dati relativi a persone identificabili quando le finalità del trattamento possono essere raggiunte impiegando dati anonimi; il sistema di videosorveglianza è configurato in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati.

Principio di proporzionalità: il sistema di videosorveglianza è attivato solo quando altre misure di prevenzione, quali ad esempio i controlli da parte di addetti, i sistemi di allarme, le misure fisiche di protezione degli ingressi o le abilitazioni all'accesso agli stessi, ecc. sono state ponderatamente valutate insufficienti o inattuabili. Particolare attenzione deve essere posta alla ripresa di luoghi privati o di accessi a edifici, ed all'eventuale duplicazione delle immagini registrate. Il criterio di proporzionalità deve essere rispettato in ogni fase o modalità del trattamento, come ad esempio quando è necessario stabilire:

- 6.1. Se sia sufficiente, ai fini della sicurezza, rilevare immagini che non rendono identificabili i singoli cittadini, anche tramite ingrandimenti dell'immagine;
- 6.2. Se sia realmente essenziale ai fini prefissati la raccolta di immagini dettagliate;
- 6.3. La dislocazione, l'angolo visuale, l'uso di zoom automatici e le tipologie - fisse o mobili - delle apparecchiature;
- 6.4. Quali dati rilevare, se registrarli o meno, se avvalersi di una rete di comunicazione o creare una banca di dati, indicizzarla, utilizzare funzioni di fermo-immagine o tecnologie digitali, abbinare

altre informazioni o interconnettere il sistema con altri sistemi gestiti dallo stesso titolare o da terzi;

- 6.5. La durata dell'eventuale conservazione (che, comunque, deve essere sempre limitata temporalmente).

Principio di finalità: il sistema di videosorveglianza deve essere utilizzato solo ed esclusivamente per gli scopi istituzionali dell'Ente, indicati nel presente articolo.

4. Articolo 4 – Caratteristiche tecniche del sistema di videosorveglianza

1. Le caratteristiche tecniche del sistema di videosorveglianza comunale, le misure di sicurezza applicate, i soggetti (anche terzi) coinvolti nel trattamento, sono descritte all'interno della specifica "Valutazione d'impatto sulla protezione dei dati" (cd DPIA) ai sensi dell'art. 35 del Reg. 679/2016.
2. In ragione della delicatezza delle informazioni contenute, la DPIA non sarà oggetto di pubblicazione nel sito web istituzionale.

5. Articolo 5 Accordo di contitolarità dei dati

- 1) I Comuni che hanno trasferito la funzione di Polizia Locale riconoscono che le attività di trattamento dei dati relative al progetto di videosorveglianza sono svolte in regime di contitolarità ai sensi dell'art. 26 del GDPR, avendone congiuntamente determinato finalità e mezzi. Qualora per lo svolgimento delle attività di trattamento in oggetto sia necessario che le Parti condividano software ed account in gestione al Comune, si conviene che anche tali strumenti siano disciplinati dall'accordo di contitolarità senza la necessità di ulteriori accorgimenti.
- 2) I Comuni che hanno trasferito la funzione di Polizia Locale e la Comunità determinano che i dati personali trattati singolarmente, quali titolari autonomi, o congiuntamente, quali contitolari, dovranno essere conformi a finalità di carattere istituzionale o comunque alle finalità previste da norme di legge o regolamento, previa verifica dei requisiti di liceità di cui all'art. 6 del Reg. 679/16.
- 3) La Comunità Riviera Friulana gestisce, per conto dei Comuni che hanno trasferito la funzione di Polizia Locale, i sistemi di videosorveglianza da essi attivati o sul cui territorio sono installati i dispositivi di ripresa;
- 4) I Comuni e la Comunità Riviera Friulana sottoscriveranno apposito accordo di contitolarità da approvarsi in Giunta Comunale e Comitato esecutivo, dove saranno definiti gli aspetti derivanti dall'accesso alle sedi, la manutenzione degli impianti, la gestione delle richieste di esercizio dei diritti ed altre richieste dell'Interessato, la gestione delle richieste di risarcimento danni, la gestione dei rapporti con l'Autorità Garante per la protezione dei dati personali, la trasparenza e l'informativa nei confronti degli interessati.

6. Articolo 6 – Condivisione e accesso al Sistema di videosorveglianza da parte di soggetti terzi

1. In ottemperanza al principio di economicità delle risorse e dei mezzi impiegati, è ammesso l'accesso e la gestione del Sistema di videosorveglianza da parte di soggetti terzi nelle forme e modalità di seguito descritte:
 - a) Comunità Riviera Friulana conferisce, tramite apposito atto, ad un altro ente o soggetto privato la gestione del sistema per conto della Comunità;
 - b) Comunità Riviera Friulana gestisce, in forza di specifica convenzione, congiuntamente o per conto di altri comuni o enti, sistemi di videosorveglianza da essi attivati o sul cui territorio sono installati i dispositivi di ripresa;

- c) Comunità Riviera Friulana mette a disposizione, previa stipula di apposita convenzione o accordo, a Forze di Polizia ed Autorità esterne l'utilizzabilità e l'accesso al Sistema di videosorveglianza.

7. Articolo 7 – Titolarità del trattamento dei dati personali nei sistemi di videosorveglianza

1. Il titolare del trattamento è la Comunità Riviera Friulana rappresentata dal Presidente quale legale rappresentante *pro tempore*, salvo diverse indicazioni riportate negli accordi o convenzioni predisposte nelle ipotesi di condivisione del Sistema di videosorveglianza di cui al precedente art. 6.

8. Articolo 8 – Valutazione d'impatto sulla protezione dei dati personali e consultazione preventiva con l'Autorità di Controllo

1. La Comunità Riviera Friulana nella sua qualità di titolare del trattamento dei dati personali adempie all'obbligo previsto dall'art. 35 Reg. Eu 679/2016 in tema di valutazione d'impatto sulla protezione dei dati personali.
2. Il titolare del trattamento consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati ai sensi del suindicato art. 35 presenti un rischio elevato per i diritti e le libertà delle persone fisiche, in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; osserva in ogni caso integralmente quanto previsto dall'art. 36 del medesimo regolamento comunitario.

9. Articolo 9 – Referente interno del sistema di videosorveglianza

1. La Comunità Riviera Friulana, nella persona del legale rappresentante, designa e nomina con apposito atto, quale Referente interno del sistema di videosorveglianza il Comandante della Polizia Locale o altra persona individuata dal titolare che per esperienza, capacità professionale ed affidabilità fornisce idonea garanzia in merito alla corretta gestione del sistema di videosorveglianza e del trattamento dei dati che esso comporta.
2. Il Referente interno del sistema di videosorveglianza sovrintende alla gestione tecnica e giuridica del sistema secondo quanto previsto nell'atto di designazione.
3. Il Referente interno del sistema di videosorveglianza procede ad effettuare le attività di sua competenza attenendosi alle istruzioni impartite dal titolare tramite l'atto di designazione o in successive comunicazioni, avendo in ogni caso cura di rispettare quanto previsto dalla normativa vigente in materia di trattamento dati personali.
4. Il Referente interno del sistema di videosorveglianza si consulta e collabora con il Responsabile della Protezione dei dati (DPO - Data Protection Officer), individuato dall'Ente ai sensi degli art. 37 e ss. del Regolamento Europeo 679/2016, per ogni questione legata al trattamento dati personali effettuato attraverso i dispositivi di ripresa.
5. Il Referente interno del sistema può disciplinare il corretto utilizzo degli strumenti di ripresa adottati dalla Comunità Riviera Friulana attraverso specifiche procedure e disciplinari anche tenuto conto delle indicazioni dell'Autorità Garante privacy.
6. Il Referente interno del sistema ha la facoltà di nominare un proprio delegato per funzioni specifiche della gestione della videosorveglianza. Tale nomina deve essere scritta e limitata a specifiche funzioni richiamate nell'atto di nomina.

10. Articolo 10 – Amministratore di sistema del sistema di videosorveglianza

1. Nel caso in cui, all'interno del personale della Comunità vi siano soggetti che per capacità professionale ed affidabilità risultino idonei a garantire la corretta gestione tecnica del sistema di videosorveglianza e del trattamento dei dati che esso comporta, la Comunità Riviera Friulana oppure il Referente interno

del sistema di videosorveglianza, può designare e nominare con apposito atto uno o più amministratori di sistema per la gestione tecnica dell'impianto di videosorveglianza.

2. L'amministratore di sistema dell'impianto di videosorveglianza designato deve operare secondo quanto indicato nell'atto di designazione ed in conformità alle disposizioni del presente regolamento. In particolare, egli dovrà:
 - Adottare tutte le misure di sicurezza necessarie per i sistemi da lui gestiti.
 - Impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici.
 - Predisporre e verificare il corretto funzionamento dei sistemi di backup centralizzati, adottando idonee procedure per la custodia delle copie di sicurezza dei dati e delle applicazioni, nonché per il ripristino della disponibilità dei dati e dei sistemi, verificando periodicamente la leggibilità e l'integrità dei dati contenuti nelle copie di backup, effettuandone il ripristino.
 - Adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici, atti a mantenere la completezza e l'inalterabilità dei log. Tali registrazioni dovranno avere e mantenere le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità.
 - Suggestire al Titolare del Trattamento o al Referente interno l'adozione e l'aggiornamento delle misure di sicurezza atte a garantire un livello di sicurezza adeguato.
3. In ogni caso, i compiti affidati all'amministratore di sistema dell'impianto di videosorveglianza, sono analiticamente specificati con apposito atto di designazione.
4. Nel caso in cui la Comunità Riviera Friulana non disponga di personale interno che possa assumere il ruolo di amministratore di sistema e oppure si avvalga di soggetti terzi per la gestione tecnica e manutentiva del sistema di videosorveglianza, le disposizioni dei commi precedenti possono essere inserite, quali istruzioni del trattamento, all'interno dell'apposito atto di nomina a responsabile esterno ai sensi dell'art. 28 del Reg. 679/2016.

11. Articolo 11 - Registro delle attività di trattamento

1. Viene istituito, ai sensi dell'art. 30 del Regolamento (UE) 2016/679, il Registro delle attività di trattamento relativo al sistema di videosorveglianza gestito dalla Comunità Riviera Friulana, al fine di documentare, in modo trasparente e aggiornato, la tipologia delle operazioni di trattamento dei dati personali effettuate mediante gli impianti di videosorveglianza, nonché di dimostrare la conformità ai principi di responsabilizzazione ("accountability") previsti dall'art. 5, par. 2, del GDPR.
2. Il Registro è tenuto dalla Comunità Riviera Friulana, quale soggetto responsabile della gestione tecnica del sistema, e custodito presso la sede del Comando della Polizia Locale. Il Registro può essere redatto in formato elettronico o cartaceo, purché garantisca integrità, aggiornamento, completezza e disponibilità.
3. La responsabilità della tenuta e dell'aggiornamento compete al Referente per la Videosorveglianza designato dalla Comunità, sotto la vigilanza del Responsabile del trattamento e con il supporto del Data Protection Officer (DPO).
4. Il Registro contiene almeno le seguenti informazioni:
 - il nome e i dati di contatto dei Contitolari del trattamento e, se del caso, del loro rappresentante e del DPO;
 - le finalità del trattamento;
 - la descrizione delle categorie di interessati e delle categorie di dati personali trattati (immagini, targhe, metadati, ecc.);

- le categorie di destinatari a cui i dati personali sono stati o possono essere comunicati, comprese le Forze dell'Ordine e i responsabili esterni;
 - ove applicabile, i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali;
 - i termini di conservazione delle immagini e delle registrazioni;
 - la descrizione generale delle misure tecniche e organizzative di sicurezza adottate (controllo accessi, cifratura, log, backup, ecc.);
 - eventuali riferimenti a valutazioni d'impatto (DPIA), data breach e interventi correttivi.
5. Il Registro è aggiornato ogniqualvolta intervengano modifiche rilevanti alle modalità del trattamento, alla tecnologia impiegata o ai soggetti coinvolti. Il DPO verifica periodicamente la completezza e l'attualità del Registro, proponendo eventuali modifiche o integrazioni ai Contitolari. Le verifiche e gli aggiornamenti devono essere documentati e conservati agli atti della Comunità per almeno cinque anni.
 6. Il Registro e tutta la documentazione connessa sono conservati in modo sicuro per tutta la durata di utilizzo del sistema di videosorveglianza e, comunque, per un periodo non inferiore a cinque anni dall'ultima registrazione o aggiornamento. Alla cessazione del trattamento o dismissione dell'impianto, il Registro viene archiviato e conservato dalla Comunità quale documentazione ufficiale di accountability.

12. Articolo 12 – Gestione violazione della sicurezza - data breach

1. La Comunità non appena viene a conoscenza o ragionevolmente ritiene di esser venuto a conoscenza di una violazione dei dati personali, attivi senza indebito ritardo il processo di gestione della violazione.

13. Articolo 13 - Personale autorizzato al trattamento e persone autorizzate ad accedere ai locali

1. Il Referente interno del sistema designa con apposito atto, ai sensi dell'art. 2 quaterdecies del D.lgs 196/03, le persone autorizzate/incaricate al trattamento dati di videosorveglianza individuati tra gli operatori di Polizia Locale o altro personale che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
2. L'accesso alla sala di controllo è consentito esclusivamente al Titolare o al suo delegato, al Referente interno del sistema, ai soggetti autorizzati ed all'amministratore di sistema dell'impianto di videosorveglianza. Nel caso in cui la sala di controllo sia gestita da un soggetto terzo, l'accesso ai locali è disciplinato, di comune accordo, dal Referente interno e dal soggetto terzo.
3. In aggiunta ai soggetti di cui sopra, può essere autorizzato l'accesso alla sala di controllo al personale addetto alla manutenzione degli impianti ed alla pulizia dei locali, al personale delle Forze dell'Ordine ed Autorità esterne.
4. Nel caso in cui pervengano istanze di accesso, in visione, delle immagini riprese dal sistema di videosorveglianza da parte di soggetti privati (es. cittadini), l'accesso alla sala di controllo degli stessi dovrà essere annotato all'interno di un apposito registro cartaceo o informatico. Nel caso di accesso ai dati da parte dell'interessato, questi avrà visione solo alle immagini pertinenti e non eccedenti che lo riguardano.
5. Non potranno essere rilasciate copie delle immagini registrate concernenti altri soggetti diversi dall'interessato, salvi i casi di legge, in cui prevale l'interesse a conoscere l'identità dei terzi ripresi.

14. Articolo 14 - Persone autorizzate ad accedere ai dispositivi di ripresa installati sul territorio

1. L'accesso ai siti ed ai dispositivi di ripresa del sistema di videosorveglianza è consentito solamente ai soggetti autorizzati dal Titolare o dal Referente interno. Eventuali accessi da parte di persone diverse devono avvenire alla presenza dei soggetti già designati e/o autorizzati.

15. Articolo 15 - Nomina a responsabile ai sensi dell'art. 28 Reg. Eu. 679/2016 per interventi tecnici sul sistema di videosorveglianza

1. Il Referente del sistema, qualora si rendesse necessario un intervento sul sistema di videosorveglianza da parte di soggetti terzi, può avvalersi di personale esterno appositamente incaricato.
2. Laddove ne sussistano i presupposti, tale soggetto sarà nominato responsabile esterno ai sensi dell'art. 28 Reg. EU 679/2016.

16. Articolo 16 – Individuazione luoghi di ripresa e conservazione dati

1. L'individuazione dei luoghi da sottoporre a videosorveglianza, come anche previsto dal D.L. n. 11 del 2009 convertito in L. n. 38 del 2009 e nel rispetto delle finalità previste dal presente documento, compete all'Assemblea di Comunità sede di prima approvazione del presente regolamento. L'indicazione iniziale dell'ubicazione dei dispositivi di ripresa è disponibile nell'allegato A che viene approvato unitamente al presente regolamento.
2. In caso di eventuale incremento dimensionale dell'impianto, modifica o cessazione di punti di ripresa, si procederà con atto amministrativo del Referente interno del sistema di videosorveglianza in attuazione degli indirizzi della Conferenza della Polizia Locale, adottato con atto specifico del Comitato Esecutivo, nel rispetto della normativa vigente. L'indicazione dell'ubicazione delle apparecchiature viene mantenuto aggiornato dal Referente interno del sistema o dal titolare del trattamento.
3. I dati personali trattati attraverso il sistema di videosorveglianza hanno quale presupposto di liceità l'art. 6 del Reg. EU 679/2016 ed il D.lgs. 196/2003, così come modificato dal D.lgs. 101/2018. Tutti i dati saranno trattati per le finalità di cui al precedente articolo 3 del presente regolamento e per ulteriori finalità di rilevante interesse pubblico individuate da norma di legge, di regolamento o da atti amministrativi generali.
4. Il sistema di videosorveglianza, per impostazione predefinita, registra e conserva le immagini per un periodo non superiore a 7 (sette) giorni successivi alla rilevazione. Termini diversi di conservazione sono ammessi se previsti da norme di legge o da atto amministrativo motivato del Referente interno del sistema.
5. In ogni caso i soggetti autorizzati possono conservare le immagini o i filmati per periodi superiori qualora ciò sia utile per lo svolgimento di attività istruttorie o di indagine oppure in caso di specifiche richieste da parte di soggetti terzi.

17. Articolo 17 - Prescrizioni da adottare per i dati trattati

1. I monitor del sistema di videosorveglianza ed i monitor dai quali è possibile visionare i dati acquisiti con sistemi di rilevamento targhe, "Body Cam", "Dash Cam", "Droni", "Fototrappole", sono collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.
2. L'accesso alle immagini da parte del Referente interno del servizio e delle persone autorizzate al trattamento dei dati si limita alle attività oggetto della sorveglianza; eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione.

3. Nel caso in cui le immagini siano conservate all'interno di supporti di archiviazione fisici del Titolare, essi vengono custoditi, per l'intera durata della conservazione, in un armadio o simile struttura dotato di serratura, apribile solo dal dagli incaricati del trattamento dei dati.
4. La cancellazione delle immagini è garantita mediante gli strumenti e le procedure tecnologiche più avanzate; le operazioni di cancellazione devono essere effettuate esclusivamente dai soggetti autorizzati.
5. Nel caso il supporto debba essere sostituito per eccessiva usura, sarà distrutto in modo da renderlo inutilizzabile, non permettendo il recupero dei dati in esso presenti.

18. Articolo 18 - Informazioni rese al momento della raccolta

1. Nei siti oggetto di ripresa, in ottemperanza a quanto previsto dall'art. 13 del Reg. EU 679/2016 e dalle indicazioni dell'Autorità Garante per la protezione dei dati personali in materia di videosorveglianza, è installata adeguata segnaletica che informi i cittadini della presenza dei dispositivi di ripresa e delle finalità perseguite.
La segnaletica:
 - 1.1. Deve essere collocata nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con i dispositivi di ripresa;
 - 1.2. Deve avere un formato ed un posizionamento tale da essere visibile dal cittadino;
 - 1.3. Deve fornire le informazioni sul trattamento dati in maniera chiara, sintetica e senza ambiguità.
2. Presso i locali della Comunità Riviera Friulana e/o sul sito internet istituzionale, viene resa disponibile un'informativa estesa sul trattamento di videosorveglianza, redatta ai sensi dell'art. 13 Reg. EU 679/2016.

19. Articolo 19 – Accesso alle immagini del sistema di videosorveglianza

1. È garantito il diritto di accesso ai documenti elettronici contenenti video e ad ogni altro documento entro i limiti della L. 241/1990 e del Regolamento di accesso agli atti ovvero di ogni altra normativa in materia di accesso.
2. Sono altresì garanti i diritti degli interessati come previsto dagli artt. 15 e seguenti del Reg. 679/2016. In particolare, l'interessato ha altresì diritto:
 - 2.1. Di chiedere in ogni momento la conferma dell'esistenza di trattamenti che possono riguardarlo nonché l'accesso ai propri dati personali, la rettifica degli stessi qualora non siano veritieri, nonché la loro cancellazione;
 - 2.2. Di richiedere la limitazione del trattamento che lo riguarda, e può opporsi allo stesso laddove sia effettuato in modo illegittimo.
3. L'apposita istanza relativa all'esercizio dei sopracitati diritti deve essere corredata di ogni informazione e documentazione utile a consentire il reperimento delle immagini ed a dare riscontro all'interessato.
4. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione secondo quanto previsto dall'art. 2 terdecies del D.lgs 196/03 e s.m.i.
5. Previa richiesta scritta, il sistema di videosorveglianza potrà essere utilizzato anche in relazione ad indagini dell'Autorità Giudiziaria, di Corpi di Polizia o da organi di Polizia Locale nello svolgimento di loro indagini o quando utili per il reperimento di informazioni ad esse collegate.

20. Articolo 20 - Comunicazioni

1. La comunicazione dei dati personali da parte della Comunità Riviera Friulana a favore di soggetti terzi, per compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, è ammessa nei limiti dell'art. 2 ter comma 2 decreto del legislativo 30 giugno 2003, n. 196, così come modificato dal D.lgs. 101/2018.

2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal responsabile e che operano sotto la loro diretta autorità.
3. È in ogni caso fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del D.lgs. 30/6/2003, n. 196, così come modificato dal D.lgs. 101/2018, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, per cui si applica il D. Lgs. 51/2018.

21. Articolo 21 – Trattamento per finalità di polizia giudiziaria

1. I trattamenti di dati personali da parte del Corpo di Polizia Locale effettuati per le finalità di polizia giudiziaria, quando direttamente correlati all'esercizio dei compiti di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria svolti ai sensi del codice di procedura penale, sono disciplinati dal **Decreto del Presidente della Repubblica del 15 gennaio 2018, n. 15** *"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. (GU Serie Generale n.61 del 14-03-2018)* e dal **D.lgs. del 18 maggio 2018, n. 51**, recante: *"Attuazione della direttiva (UE) 2016/680 del Parlamento e del consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2018/977 GAI del Consiglio"*.

22. Articolo 22 - Pubblicità del regolamento

1. Copia del presente regolamento, a norma dell'art. 22 della legge 7 agosto 1990, n. 241, è tenuta a disposizione del pubblico perché ne possa prendere visione in qualsiasi momento.
2. Il presente regolamento verrà pubblicato all' Albo pretorio e sul sito internet istituzionale dell'Ente, nella sezione "amministrazione trasparente", ai sensi della vigente normativa in tema di pubblicazione degli atti amministrativi.

23. Articolo 23 – Sopravvenienza di nuove disposizioni normative

1. Le disposizioni del presente regolamento si intendono modificate per effetto di sopravvenute norme vincolanti statali, regionali o comunitarie.
2. In tali casi si applica la normativa sovraordinata. L'Ente potrà in ogni caso provvedere ad aggiornare il presente regolamento per renderlo maggiormente conforme alle eventuali disposizioni normative intervenute.

24. ALLEGATO A – Individuazione dei punti di ripresa

1. Allegato A