



Comune di
ORISTANO

**REGOLAMENTO
PER LA DISCIPLINA DELLA
VIDEOSORVEGLIANZA**

Approvato con Delibera del Consiglio comunale n. 46 del 30.06.2026

INDICE

<i>Premessa e riferimenti normativi</i>	<i>pag.</i>	<i>03</i>
CAPO I - PRINCIPI GENERALI	pag.	05
Art. 1 - Oggetto	pag.	05
Art. 2 - Ambito di applicazione	pag.	05
Art. 3 - Definizioni	pag.	05
Art. 4 - Finalità del trattamento dei dati personali per le attività di videosorveglianza	pag.	07
Art. 5 - Caratteristiche dei sistemi di videosorveglianza	pag.	08
CAPO II - TRATTAMENTO DEI DATI: SOGGETTI ED ADEMPIMENTI	pag.	08
Art. 6 - Titolare/contitolari del trattamento	pag.	08
Art. 7 - Delegati al trattamento	pag.	10
Art. 8 - Nomina degli incaricati e dei preposti alla gestione dell'impianto di videosorveglianza	pag.	11
Art. 9 - Persone autorizzate ad accedere alla sala di controllo	pag.	11
Art. 10 - Obblighi degli operatori	pag.	11
Art. 11 - Responsabile alla protezione dati	pag.	12
Art. 12 - Obblighi di notifica	pag.	12
CAPO III - IL TRATTAMENTO DEI DATI PERSONALI	pag.	12
Art. 13 - Raccolta e requisiti dei dati personali	pag.	12
Art. 14 - Caratteristiche dei sistemi di videosorveglianza – trasmissioni su reti	pag.	13
Art. 15 - Sicurezza del trattamento	pag.	14
Art. 16 - Valutazioni d'impatto sulla protezione dei dati	pag.	15
Art. 17 - Accertamenti di illeciti e indagini di Autorità Giudiziarie o di Polizia	pag.	15
Art. 18 - Abbandono di rifiuti	pag.	16
Art. 19 - Violazione dei dati personali	pag.	16
Art. 20 - Diritti dell'interessato	pag.	16
Art. 21 - Sistemi mobili	pag.	17
CAPO IV - DELLE TUTELE E DELLE MODIFICHE	pag.	17
Art. 22 - Informative e livelli essenziale di tutela	pag.	17
Art. 23 - Accesso alle immagini	pag.	18
Art. 24 - Sicurezza dei dati	pag.	19
Art. 25 - Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale	pag.	19
Art. 26 - Cessazione del trattamento dei dati	pag.	19
Art. 27 - Comunicazione e pubblicità	pag.	19
Art. 28 - Modifiche regolamentari	pag.	19
CAPO V - DISPOSIZIONI FINALI	pag.	19
Art. 29 - Rinvio	pag.	19
Art. 30 - Entrata in vigore e disposizioni collegate	pag.	20

Premessa e riferimenti normativi

Il Regolamento disciplina la raccolta, trattamento e conservazione dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza nel territorio del Comune di Oristano, per il tramite del Corpo di Polizia Locale, per lo svolgimento di funzioni istituzionali a fini di tutela della sicurezza urbana e nel rispetto dei diritti, delle libertà fondamentali, della dignità delle persone fisiche e con particolare riferimento alla riservatezza e all'identità personale.

Per quanto non dettagliatamente disciplinato nel presente Regolamento, si rinvia alle seguenti disposizioni:

- *Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'art. 57, D. Lgs. n. 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia".*
- *Regolamento UE n. 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.*
- *Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.*
- *D. Lgs. 30 giugno 2003, n. 196, come modificato dal D. Lgs. n. 101 del 10 agosto 2018, recante: "Codice in materia di protezione dei dati personali".*
- *D. Lgs. 18/05/2018, n. 51 recante: "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio".*
- *Artt. 50 e 54, D. Lgs. 18 agosto 2000, n. 267 e ss.mm.ii. .*
- *Decalogo del 29 novembre 2000 promosso dal Garante per la protezione di dati personali.*
- *Circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/A/471.*
- *Legge. 23 aprile 2009, n. 38, di conversione, con modifiche del D.L. 23 febbraio 2009, n. 11.*
- *Provvedimento in materia di videosorveglianza emanato dal garante per la protezione dei dati personali in data 8 aprile 2010 (G.U. N. 99, del 29/04/2010).*
- *Legge n. 125/2008 (legge conversione d.l. n. 92/2008, c.d. "decreto sicurezza").*
- *D.M. del Ministero dell'Interno 5 Agosto 2008 (G.U. N. 186, del 09/08/2008).*
- *Legge 15 luglio 2009, n. 94 - Disposizioni in materia di sicurezza pubblica.*
- *D.L. 20/02/2017, n. 14 - Disposizioni urgenti in materia di sicurezza delle città.*
- *D.L. 04/10/2018, n. 113. Disposizioni urgenti in materia di protezione internazionale e immigrazione, sicurezza pubblica, nonché misure per la funzionalità del Ministero dell'interno e l'organizzazione e il funzionamento dell'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata.*
- *Art. 615-bis, Regio Decreto 19 ottobre 1930, n. 1398 ss.mm.ii. apportate dal D. Lgs. 11 maggio 2018, n. 63, dal D. Lgs. 10 aprile 2018, n. 36 e dal D. Lgs. 1° marzo 2018, n. 21.*
- *Legge 20 maggio 1970, n. 300.*
- *Legge 7 marzo 1986 n. 65.*
- *D. Lgs. 31 marzo 1998, n. 112.*

- L. R. Sardegna 02 agosto 2007, n. 9.
- legge 3 ottobre 2025, n. 147, di conversione del Decreto-legge n. 116/2025, noto come DL Terra dei Fuochi
- *Provvedimento del Garante* per la protezione dei dati personali in materia di videosorveglianza 8 aprile 2010.
- *Circolare del Ministero dell'Interno n. 558/A421.2/70/195860*, del 06.08.2010.
- *Circolare del Ministero dell'Interno n. 558/SICPART/421.2/70/224632* del 02.03.2012.
- *D. Lgs. 10 agosto 2018, n. 101.*
- *Statuto Comunale.*
- *Regolamenti Comunali vigenti.*

CAPO I

PRINCIPI GENERALI

Art. 1 – Oggetto

Il presente Regolamento ha per oggetto la disciplina delle misure procedurali e regole di dettaglio del trattamento di dati personali, acquisiti mediante sistema di videosorveglianza, affinché ciò si svolga nel rispetto dei diritti, delle libertà fondamentali, della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Garantisce altresì i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento di dati e potrà essere integrato e/o modificato con successivo provvedimento, in caso di variazione delle condizioni di applicazione o per intervenute modifiche normative in materia di protezione dei dati personali.

Art. 2 - Ambito di applicazione

Il regolamento disciplina il trattamento di dati personali, realizzato mediante sistema di videosorveglianza, attivato nel territorio del Comune di Oristano.

L'utilizzo del sistema della videosorveglianza è attuato attraverso il corretto impiego delle applicazioni e nel rispetto dei principi di cui all'art. 5, Regolamento UE Generale sulla protezione dei dati personali 2016/679 (di seguito RGDP), ovvero:

- a) Liceità, correttezza e trasparenza, in piena ottemperanza della normativa vigente, nei confronti dell'interessato;
- b) Adeguatezza, in modo tale da essere pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- c) Integrità e riservatezza, in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- d) Proporzionalità, con sistemi attuati con attenta valutazione;
- e) Finalità, attuando il trattamento dei dati solo per scopi determinati ed espliciti;
- f) Necessità, con esclusione di uso superfluo della videosorveglianza;
- g) Pertinenza e non eccedenza: il sistema informativo e i programmi informatici (di cui al trattamento dei dati personali) sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità;

Il trattamento dei dati personali riferito agli ambiti cui si riferisce il regolamento non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni che sono assoggettate ad un regime di tipo particolare.

Art. 3 – Definizioni

Ai fini del presente regolamento si intende:

- a) Per “**banca di dati**”, il complesso di dati personali formatosi presso la Centrale Operativa/di controllo e trattato esclusivamente mediante riprese video che, in relazione ai luoghi di installazione delle videocamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate ed i mezzi di trasporto;
- b) Per “**trattamento**”, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione,

l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- c) Per “**limitazione di trattamento**”, il contrassegno dei dati personali conservati con l’obiettivo di limitarne il trattamento in futuro;
- d) Per “**archivio**”, qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- e) Per “**dato personale**”, qualsiasi informazione riguardante una persona fisica, identificata o identificabile (“interessato”). Si considera identificabile la persona fisica, che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale, come pure mediante riferimento a qualsiasi altra informazione, rilevati con trattamenti di immagini effettuati attraverso l’impianto di videosorveglianza;
- f) Per “**Titolare del trattamento**”, il Comune di Oristano, Ente locale territoriale, nelle sue articolazioni interne, cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali;
- g) Per “**Responsabile del trattamento**”, la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- h) Per “**Incaricato**”, la persona fisica o giuridica autorizzata a compiere operazioni di trattamento dei dati dal titolare del trattamento o dal delegato al trattamento;
- i) Per “**interessato**”, colui a cui si riferiscono i dati personali;
- j) Per “**violazione dei dati personali**”, la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- k) Per “**comunicazione**”, 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;
- l) Per “**diffusione**”, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- m) Per “**dato anonimo**”, il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- n) Per “**blocco**”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
- o) Per “**immagine**”, il dato trattabile con metodo analogico o digitale, costituito da una rappresentazione visiva di una persona, di un ambiente o di una cosa. L’immagine raffigurante o contenente qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale, costituisce dato personale;
- p) Per “**videosorveglianza**”, l’attività di sorveglianza effettuata mediante il trattamento di immagini e di dati ad esse intrinsecamente correlati, finalizzato alla tutela delle persone, dell’ambiente, delle attività e delle cose;
- q) Per “**Garante**”, l’autorità istituita, dalla Legge 31.01.1996 n. 675, di controllo indipendente per la protezione dei dati personali art. 14, c. 1, lett. b), D. Lgs. 10 agosto 2018, n. 101.

Art. 4 – Finalità del trattamento dei dati personali per le attività di videosorveglianza

Il trattamento dei dati personali è effettuato a seguito dell'attivazione del sistema di videosorveglianza nel territorio del Comune di Oristano e all'utilizzo di tutte le tecnologie che comportano l'utilizzo di telecamere.

Presso la Centrale Operativa e di Videosorveglianza del Corpo Polizia Locale, secondo quanto disciplinato dal regolamento, sono posizionati i *monitors* per la visualizzazione delle immagini riprese dalle telecamere di videosorveglianza, mentre in ogni ufficio, preposto al trattamento dei dati inerenti le proprie tecnologie, sono presenti i dispositivi che elaborano i dati relativi ai sistemi in dotazione.

Il trattamento dei dati, conforme alle finalità istituzionali demandate al Comune di Oristano, ed in particolare sul territorio comunale, attraverso l'acquisizione in tempo reale di dati ed immagini, si espleta per:

- a) Protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e la sicurezza pubblica, la prevenzione, accertamento o repressione dei reati, la razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti;
- b) Attività di Polizia Giudiziaria, svolte da Organi di Polizia, inerenti attività d'indagine e ai fini di prevenzione e repressione di reati;
- c) Strumento operativo di Protezione Civile;
- d) Monitoraggio delle arterie stradali a maggiore rilevanza nel territorio, a fini di prevenzione di problemi inerenti i flussi veicolari e la mobilità stradale, vigilanza del traffico ed individuazione dei luoghi ad elevata intensità che impongono il Pronto Intervento della Polizia Locale o di altre Forze di Polizia;
- e) Accertamento delle situazioni di pericolo per la sicurezza urbana connessa alla circolazione stradale, con rilevazione di situazioni di pericolo per gli utenti della strada, e individuazione di comportamenti di guida non rispettosi del Codice della Strada tali da pregiudicare la sicurezza stradale, che impongono l'intervento degli operatori in casi di pericolo o di sinistri stradali;
- f) Accertamento di infrazioni al Codice della Strada, in particolare con strumentazioni di videosorveglianza atte a rilevare: limiti di velocità, accessi alla ZTL (zona a traffico limitato), coperture assicurative e revisioni, infrazioni semaforiche;
- g) Sorveglianza di particolari aree e siti ad alto rischio di alterazione degli equilibri ambientali;
- h) Controllo di situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertamenti su aree su cui insistono fenomeni incontrastabili di deposito/discarica di materiali e/o sostanze pericolose, di rilevanza penale o amministrativa;
- i) Tutela degli immobili di proprietà o in gestione dell'Amministrazione Comunale e prevenzione di eventuali atti di vandalismo o danneggiamento del patrimonio pubblico, a garanzia della sicurezza negli ambienti circostanti, nelle piazze, scuole, parchi, parcheggi, complessivamente della proprietà pubblica e privata soggetta al pubblico utilizzo, accertando e reprimendo eventuali reati al fine di una migliore razionalizzazione dei servizi offerti all'utenza, in funzione di far crescere la percezione di sicurezza, nel pieno rispetto delle competenze attribuite dalla legge all'Ente locale Comune;
- j) Rilevamento di situazioni di occupazione abusiva del suolo pubblico e di disturbo alla quiete pubblica;
- k) Acquisizione prove pertinenti e rilevanti, idonee a dimostrare l'esistenza del fatto storico da provare;

Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese della videosorveglianza e che, in relazione ai luoghi di

installazione delle videocamere, interesseranno i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata e comunque solo i dati strettamente necessari per il raggiungimento delle finalità perseguite.

Art. 5 - Caratteristiche dei sistemi di videosorveglianza

Il sistema è composto da una Centrale Operativa, con funzioni di controllo e supervisione, collocata presso il Comando Polizia Locale, di *servers* per la registrazione delle immagini collocati presso i locali del Comando suddetto e da un insieme di punti di ripresa costituiti da telecamere fisse e/o brandeggiabili, o telecamere mobili (foto-trappole, *bodycam*, *dashcam*, droni) dislocate nel territorio comunale.

Le immagini videoriprese dalle telecamere sono trasmesse alla Centrale Operativa della Polizia Locale tramite diverse infrastrutture: un'infrastruttura di rete in fibra ottica, dedicata esclusivamente a tale servizio; tramite collegamento a un'infrastruttura di rete MAN; tramite sistemi *wireless*; per mezzo di router in 4 o 5 G o tramite fibra ottica di internet service providers, con trasmissione di tipo digitale ed *encryption* dei dati e/o VPN.

Le immagini relative alle infrazioni dei sistemi a varco della ZTL, dei rilevatori di velocità e di infrazioni al codice della strada, possono confluire direttamente in archivi dei rispettivi Servizi o Uffici di competenza.

Il sistema di videosorveglianza cittadino è isolato dagli altri sistemi informatici comunali e da altri sistemi di soggetti pubblici e non è connesso ad alcuna rete pubblica di telecomunicazioni priva di protezioni informatiche adeguate. Non è quindi accessibile da altre periferiche oltre che dalla Centrale Operativa o dalle Sale Operative delle Forze di Polizia. Tuttavia, nel presente Regolamento, è previsto e disciplinato che, nel caso in cui il sistema di videosorveglianza comunale venga integrato con sistemi esterni di altri Enti o aperto ad accessi esterni delle Forze di Polizia, ciò avvenga a condizione che sia puntualmente disciplinato da appositi Patti per la Sicurezza o da atti con rilevanza giuridica tra le parti, previa redazione di disciplinari e la sottoscrizione di protocolli d'intesa come indicato nell'art.6

La visualizzazione in diretta delle immagini rilevate con i sistemi di videosorveglianza nella sala della Centrale Operativa è focalizzata su obiettivi particolarmente sensibili e strategici per la sicurezza urbana e/o in presenza del requisito di pubblico interesse, nel pieno rispetto dell'ambito di applicazione disciplinato dall'art. 3 del presente regolamento e di non eccedenza dei dati o dei trattamenti.

CAPO II

TRATTAMENTO DEI DATI: SOGGETTI E ADEMPIMENTI

Art. 6 – Titolare/contitolari del trattamento

Il Comune di Oristano è il Titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Titolare, ai sensi dell'art. 2-*quaterdecies* D. Lgs. 10 agosto 2018, n. 101, delega le relative funzioni al Dirigente della Polizia Locale per quanto riguarda l'impianto di videosorveglianza di Sicurezza Urbana; può delegare altri Dirigenti dei servizi competenti per le telecamere a tutela del patrimonio immobiliare comunale o aree di sua proprietà non collegate e/o connesse alla Centrale Operativa della Polizia Locale.

Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli artt. 15-22

RGD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), nel Piano Esecutivo di Gestione e/o nel PIAO, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Il Titolare adotta misure appropriate, mediante informative estese pubblicate anche sul sito web dell'Ente ed informative sintetiche apposte su cartelli posti in corrispondenza delle aree video-sorvegliate, per fornire all'interessato:

- a) Le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
- b) Le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato;

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali, di seguito indicata con "DPIA", ai sensi dell'art. 35 RGPD, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

In ogni caso l'Ente, alla luce di quanto indicato nel provvedimento "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018), provvede a dare evidenza dell'analisi dei rischi eseguita sugli impianti in uso alla data di approvazione del presente regolamento.

Il Titolare indica il Dirigente della Polizia Locale quale soggetto competente all'attuazione del presente regolamento e delle disposizioni che disciplinano l'attività di Videosorveglianza del Comune, il quale designerà ed autorizzerà con proprio provvedimento i Responsabili e i Funzionari delle singole strutture in cui si articola l'organizzazione comunale della Polizia Locale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza.

Qualora sia necessario avvalersi per l'attività di videosorveglianza di responsabili del trattamento ex art. 28 del GDPR, il Dirigente della Polizia Locale provvede a nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

Possono essere individuati dal Comune ulteriori designati in ragione di necessità o esigenze specifiche.

Con l'atto di designazione, ai singoli autorizzati, sono affidati compiti specifici e puntuali prescrizioni per l'utilizzo dei sistemi in conformità ai principi enunciati nel presente regolamento.

Gli autorizzati alla gestione dell'impianto sono nominati dal Dirigente nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio.

Il Dirigente designa gli amministratori di sistema della Videosorveglianza comunale mediante un atto che reca le specifiche istruzioni e gli obblighi posti in capo dal Titolare e dalla vigente normativa per coloro che rivestono tale funzione nell'Ente pubblico.

Le modalità per la nomina dei soggetti designati, autorizzati, amministratori di sistema interno od esterno, sono individuate nel modello organizzativo in materia di protezione dei dati personali di cui ai successivi artt. 7 e 8.

Allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD.

In caso di Contitolarità, Titolarità autonoma o nomina del Comune di Oristano a Responsabile del trattamento dei dati raccolti tramite sistema di videosorveglianza, gli obblighi e i reciproci rapporti con contitolari e titolari saranno disciplinati nell'ambito dei Patti per la sicurezza siglati con le Forze di Polizia dello Stato, protocolli d'intesa ovvero altri atti giuridicamente vincolanti tra Enti, in cui sia specificato, tra le altre cose, che l'accesso alle immagini delle telecamere potrà avvenire anche dalle sale operative dei diversi soggetti, previa redazione di un disciplinare.

Il Titolare, inoltre, assicurerà che gli impianti di videosorveglianza non siano utilizzati, in base all'art. 4 dello statuto dei lavoratori (Legge n. 300 del 20 maggio 1970 e ss.mm.ii.), per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati, fatte salve le richieste dell'Autorità Giudiziaria.

Art. 7 - Delegati al trattamento

Un Dirigente è nominato Delegato al trattamento e deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.

I delegati al trattamento sono designati, di norma, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

- a) La materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- b) Il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- c) Gli obblighi ed i diritti del Titolare del trattamento;

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun Delegato.

Il Titolare può avvalersi per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al c. 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi ed i diritti del responsabile al trattamento e le modalità di trattamento.

Gli atti che disciplinano il rapporto tra il Titolare ed il responsabile al trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

È consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-delegato.

Il Delegato al trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

Il Delegato al trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- a) Alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- b) All'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- c) Alla sensibilizzazione e formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- d) Alla designazione del Responsabile per la Protezione dei Dati (DPO), se a ciò demandato dal Titolare;
- e) Ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati, di seguito indicata con "DPIA", fornendo allo stesso ogni informazione di cui è in possesso;
- f) Ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati;

Il Delegato del trattamento, ha l'onere di custodire le chiavi per l'accesso a locali e/o ove sono custoditi i *servers*, nonché le *password* per l'accesso ed utilizzo dei sistemi informatici.

Art. 8 – Nomina degli incaricati e dei preposti alla gestione dell'impianto di videosorveglianza

Il Dirigente delegato designa e nomina i preposti in numero sufficiente a garantire la gestione del servizio di videosorveglianza nell'ambito del personale dell'Ente, che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati; inoltre conferisce incarico a tutti gli operatori che in via principale o residuale effettuano o dovranno effettuare un trattamento dei dati.

La gestione dell'impianto di videosorveglianza è riservata al personale appartenente all'Ente.

Con l'atto di nomina, ai singoli preposti saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi e, prima dell'utilizzo degli impianti, saranno istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento.

Art. 9 – Persone autorizzate ad accedere alla sala di controllo

I monitor degli impianti di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini a persone estranee non autorizzate. L'accesso alla sala di controllo è consentito solamente al personale dell'Ente, autorizzato dal Dirigente del Settore Polizia Locale delegato al trattamento, di cui ai successivi punti.

Sono autorizzati all'accesso ai locali:

- a) incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità di cui al presente regolamento;
- b) il personale delle forze dell'ordine impegnato nei propri servizi d'istituto;
- c) il personale deputato agli interventi di manutenzione;
- d) il personale addetto alla pulizia dei locali;
- e) altro personale autorizzato dal Dirigente o dal Funzionario Incaricato.

Art. 10 - Obblighi degli operatori

L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolga nei luoghi pubblici mentre esso non è ammesso nelle proprietà private, fatte salve le richieste dell'Autorità giudiziaria. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente art. 11, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 c. 3.

Art. 11 – Responsabile della protezione dati

Il Responsabile alla protezione dei dati, in seguito indicato con “DPO”, viene designato dal Titolare sulla base degli artt. 37-39 del GDPR, quale soggetto in possesso di idonee qualità professionali e con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati e di capacità di promuovere la cultura della protezione dati all’interno dell’organizzazione comunale. Il Titolare ed il Dirigente provvedono affinché il DPO mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione. Nel caso in cui il DPO non sia un dipendente dell’Ente, l’incaricato persona fisica è selezionato fra soggetti aventi le medesime qualità professionali richieste al dipendente, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili; i compiti attribuiti al DPO sono indicati in apposito contratto di servizi. Il DPO esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare ed al Delegato al trattamento.

Il Titolare ed il Delegato al trattamento assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Nello svolgimento dei compiti affidatigli, il DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell’ambito di applicazione, del contesto e delle finalità del medesimo.

Ferma restando l’indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare del trattamento.

Art. 12 – Obblighi di notifica

Il Comune di Oristano, quale Titolare del trattamento dei dati personali rientrante nel campo di applicazione del presente regolamento, adempie agli obblighi di notificazione preventiva al Garante per la protezione dei dati personali. I dati trattati devono essere notificati al Garante solo se rientrano nei casi specificatamente previsti dalla normativa vigente sulla protezione dei dati personali; le disposizioni vigenti prevedono che non vanno comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardano immagini o suoni conservati temporaneamente per esclusiva finalità di sicurezza o di tutela delle persone e del patrimonio.

CAPO III

IL TRATTAMENTO DEI DATI PERSONALI

Art. 13 - Raccolta e requisiti dei dati personali

I dati personali oggetto di trattamento sono:

- a) Trattati in modo lecito e secondo correttezza;
- b) Raccolti e registrati per le finalità di cui al presente regolamento e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi attuali e, se necessario, aggiornati;
- c) Raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;

- d) Conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dal successivo c. 5;

I dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza, installate in corrispondenza di intersezioni, piazze, parchi pubblici e immobili, nel territorio comunale.

Le telecamere consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario. Tali caratteristiche tecniche consentono un significativo grado di precisione e di dettaglio della ripresa. Sono utilizzate sia telecamere di contesto che telecamere Ocr – Anpr per la lettura delle targhe dei veicoli.

L'uso di sistemi di Intelligenza Artificiale avviene nel rispetto dell'AI ACT e degli obblighi di valutazione dei rischi, trasparenza e formazione specifica del personale.

Le attività di videosorveglianza sono finalizzate alla tutela della sicurezza urbana e, come disposto dalla normativa in materia, il termine massimo di durata della conservazione dei dati è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte, fatte salve specifiche esigenze di ulteriore conservazione.

La congruità di un termine di tempo più ampio di conservazione andrà adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'Autorità Giudiziaria o dalla Polizia Giudiziaria in relazione ad un'attività investigativa in corso e compatibilmente con la disponibilità di spazio disco sui servers.

Il sistema impiegato è programmato in modo da operare, al momento prefissato, l'integrale cancellazione automatica delle informazioni, allo scadere del termine previsto da ogni supporto, mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Art. 14 – Caratteristiche dei sistemi di videosorveglianza – trasmissione su reti

MAN: Per facilitare l'interconnessione dei sistemi di videosorveglianza viene utilizzata, oltre che la rete in fibra ottica proprietaria e dedicata, anche la *MAN (Metropolitan Area Network)* del Comune di Oristano. La tecnica utilizzata per indirizzare il flusso video al sistema centrale di registrazione è il *VRF (Virtual Routing and Forwarding)*, tecnologia che, in una rete *MPLS*, consente di distinguere flussi di traffico differenti perché legati a tabelle di *routing* differenti con funzionalità di un router virtuale consentendo la creazione, in uno stesso *router* fisico, di un canale riservato ad altissimo livello di sicurezza.

RTR: una parte del sistema di videosorveglianza (finanziato dal Ministero degli Interni per il tramite della Regione Sardegna) potrà essere interconnesso con la Rete Telematica Regionale, ovvero l'infrastruttura di proprietà della Regione al servizio dell'Amministrazione regionale, dei suoi Enti e Agenzie e delle Aziende sanitarie per le esigenze di connettività dati e voce. La soluzione tecnica adottata dalla Regione sarà costituita da un *backbone* in fibra ottica, con nodi dislocati presso le città capoluogo di provincia, punto di raccolta per le esistenti reti metropolitane, che sfrutta tecnologie trasmissive *DWDM* per il *Backbone* e *IP/MPLS* per le sedi periferiche non direttamente interconnesse in fibra ottica e *Gigabit Ethernet* per le *MAN*.

Sarà cura dell'Amministrazione Regionale predisporre un piano armonizzato tra quello comunale e quello della RTR, e occuparsi della sicurezza della rete messa a disposizione.

La RAS per poter comunicare, interagire e gestire l'hardware di sorveglianza associato al progetto, attraverso il proprio *DVMS (Digital Video Management System)*, è dotata, di un software di monitoraggio, in grado di operare con gli eterogenei sistemi di videosorveglianza locali.

Il *DVMS*, è conforme alla normativa vigente sulla *privacy*, rispetta le direttive del Ministero dell'Interno, normative CEI EN 50132-1 (CEI 79-70) Sistemi di allarme Sistemi di videosorveglianza per applicazioni di sicurezza.

I sistemi di sicurezza della RTR sono curati dalla Regione Autonoma della Sardegna, che garantirà il rispetto della normativa in materia, attraverso tecnica di VRF, creando *routers* virtuali per ogni VLAN o gruppo di VLAN o attraverso *firewall* o altra tecnologia idonea individuata.

Presso la Centrale Operativa è possibile visualizzare le immagini in diretta e registrate di tutte le telecamere, brandeggiare (in orizzontale ed in verticale) e zoomare gli obiettivi delle telecamere.

Modifiche tecniche al sistema di videosorveglianza, conseguenti alle necessarie ed inevitabili innovazioni tecnologiche, ivi compresa l'integrazione con sistemi di AI, potranno essere adottate previo aggiornamento/stesura delle presupposte valutazioni di impatto facendo ricorso ad allegati tecnici di volta in volta approvati, che costituiranno parte integrante e sostanziale del presente regolamento.

Per tutte le finalità di cui all'art. 4, è espressamente prevista la possibilità di un'integrazione del sistema comunale con altri sistemi e altre reti di proprietà di altri enti pubblici o privati, previa redazione/aggiornamento di DPIA e previa sottoscrizione dei già citati patti, accordi e/o protocolli d'intesa nonché di disciplinari tecnici che definiscano e regolamentino gli aspetti di responsabilità e le modalità tecnico-operative e di sicurezza informatica.

Art. 15 - Sicurezza del trattamento

Il Comune di Oristano e ciascun Delegato al trattamento, mettono in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione (compatibilmente con le risorse messe a disposizione dall'Ente), nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Delegato al trattamento:

- a) Sistemi di autenticazione, sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- b) Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati

o ad un meccanismo di certificazione approvato. L'adozione di adeguate misure di sicurezza è lo strumento e condizione fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto 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. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

Il Comune di Oristano, e ciascun Delegato al trattamento delegato si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

I nominativi ed i dati di contatto del Titolare, e dei Delegati al trattamento ed alla protezione dati sono pubblicati sul sito istituzionale del Comune, sezione *Amministrazione Trasparente*.

Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico prevista dal D.Lgs. 10 agosto 2018, n. 101.

Art. 16 - Valutazioni d'impatto sulla protezione dei dati

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento stesso, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6 RGDP.

In ogni caso l'Ente provvede a dare evidenza dell'analisi dei rischi eseguita sugli impianti in uso alla data di approvazione del presente regolamento.

La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche.

Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa; lo stesso può affidare la redazione della DPIA ad un altro soggetto, interno o esterno al Comune. Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA. Il Delegato al trattamento deve assistere il Titolare nella redazione della DPIA fornendo ogni informazione necessaria. Il delegato della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

Il DPO può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Sia il delegato della sicurezza dei sistemi informativi se nominato, che l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

Art. 17 - Accertamenti di illeciti e indagini di Autorità Giudiziaria o di Polizia

Ove dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, l'incaricato od il Delegato della videosorveglianza provvederà a darne immediata comunicazione agli uffici in base alla competenza.

In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa disciplinate nel presente regolamento, l'incaricato procederà alla registrazione delle stesse su supporti digitali.

Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di Polizia dello Stato, Polizia Locale e l'Autorità Giudiziaria.

L'apparato di videosorveglianza potrà essere utilizzato anche in relazione ad indagini delegate dall'Autorità Giudiziaria.

Nel caso in cui gli organi della Polizia dello Stato, Polizia Locale, e A.G. nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate che sono contenute nelle riprese effettuate dal soggetto/Ente convenzionato, possono farne richiesta scritta e motivata indirizzata al Delegato della gestione e del trattamento dei dati.

Art. 18 – Abbandono di rifiuti

In relazione alla incontrollabilità del fenomeno dell'abbandono di rifiuti e delle conseguenti rilevanze penali di cui T.U Ambientale (D. Lgs. n. 152/2006 e ss.mm.ii.), nonché per effetto della legge 3 ottobre 2025, n. 147, di conversione del Decreto-legge n. 116/2025, noto come DL Terra dei Fuochi, in applicazione dei richiamati principi di liceità, finalità e proporzionalità sull'utilizzo di sistemi di videosorveglianza, risultano consentite le attività di controllo volte ad accertare violazioni del codice della strada e amministrative nel rispetto del GDPR.

Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, Legge 24 novembre 1981, n. 689 e ss.mm.ii.).

Il Comune di Oristano potrà avvalersi di un impianto di videosorveglianza mobile o "foto trappole" per controllare particolari situazioni di degrado quali l'abbandono di rifiuti su aree pubbliche e nei parchi.

Art. 19 - Violazione dei dati personali

Per violazione dei dati personali, di seguito definito come "*data breach*", s'intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal soggetto/Ente convenzionato.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy.

La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Delegato al trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, inoltre, anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio.

Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art. 20 - Diritti dell'interessato

In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, questi ha diritto:

- a) Di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;

- b) Di essere informato sugli estremi identificativi del titolare e del delegato oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
- c) Di ottenere, a cura del delegato, senza ritardo e comunque non oltre 30 giorni dalla data di ricezione della richiesta, ovvero di 90 giorni previa comunicazione all'interessato se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo:
 - I. La conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento; la richiesta non può essere inoltrata dallo stesso soggetto se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi;
 - II. La cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
 - III. Di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Per ciascuna delle richieste di cui al c. 1, lett. c), n. I), può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, definiti con atto formale dalla Giunta Comunale secondo le modalità previste dalla normativa vigente.

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.

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

Le istanze di cui al presente articolo possono essere trasmesse al titolare o al soggetto convenzionato, nominato delegato, anche mediante lettera raccomandata, posta elettronica, che dovrà provvedere in merito entro e non oltre 30 giorni.

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. 21 – Sistemi mobili

Il sistema di videosorveglianza mobile è per sua natura composto da apparati trasportabili e riposizionabili, ideali per monitorare aree periferiche del territorio non raggiungibili con sistemi di videosorveglianza tradizionale; pertanto attraverso gli strumenti denominati *body-cam* (su persona), *dash-cam* (a bordo di veicoli), o con altri sistemi mobili a posizionamento itinerante, quali foto trappole (telecamere mobili) verrà effettuato il controllo dei siti e/o delle situazioni di interesse previa adozione di appositi disciplinari e/o redazione di atti specifici.

Le riprese potranno essere effettuate anche tramite l'utilizzo di sistemi UAS (unmanned aircraft system), ovvero sistemi aerei a pilotaggio remoto che consentono un controllo del territorio avanzato. Per l'utilizzo del sistema aeromobile a pilotaggio remoto (S.A.P.R.), costituito da un aeromobile a pilotaggio remoto senza persone a bordo e dai relativi componenti necessari per il controllo e comando (stazione di controllo) da parte di un pilota remoto, saranno predisposti appositi atti e disciplinari nel rispetto delle normative vigenti e per le sole finalità consentite dalle leggi e regolamenti.

CAPO IV

DELLE TUTELE E DELLE MODIFICHE

Art. 22 – Informative e livelli essenziali di tutela

Il Comune di Oristano, in prossimità o nelle immediate vicinanze, non necessariamente a contatto con le telecamere sia fisse che mobili, delle strade, parchi e nelle piazze in cui sono posizionate le telecamere, si obbliga ad affiggere una adeguata segnaletica, che riporta la seguente dicitura *“Comune di Oristano - area videosorvegliata”* contenente l’informativa di primo livello secondo il modello allegato alle linee guida EDPB 3/2019. Tale cartello, reca il link all’informativa estesa redatta ex art. 13 del GDPR e resa disponibile dal Titolare sul sito del Comune ovvero attraverso altro canale agevolmente consultabile dagli interessati. E’ prevista l’eccezione a tale regola per il perseguimento delle finalità previste dal Reg. 680/2016 in materia di prevenzione e repressione di reati.

Art. 23 – Accesso alle immagini

Al di fuori dell’esercizio dei diritti dell’interessato ai sensi degli artt. 15-22 del GDPR, l’accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente in materia di accesso ai documenti amministrativi.

Ogni richiesta deve essere specifica, formulata per iscritto, motivata ed indirizzata al protocollo del Comune entro 3 giorni dall’evento, per consentire l’elaborazione prima della sovrascrittura dei filmati.

In linea generale l’accesso alla copia delle immagini è consentita solo previa verifica della sussistenza di un interesse qualificato ai sensi della legge 241/1990. Ogni richiesta verrà, comunque, gestita nel pieno rispetto della disciplina dell’accesso agli atti.

Non possono, di norma, essere rilasciate copie delle immagini registrate concernenti altri soggetti diversi dall’interessato, salvo casi meritevoli di tutela, motivati dal Titolare; se le immagini contengono dati riferibili a terzi, l’accesso del richiedente è consentito soltanto applicando un principio di bilanciamento ed eventualmente procedendo alla scomposizione dei dati trattati o alla privazione di alcuni elementi al fine di anonimizzare i dati di terzi per mezzo di software di elaborazione video e tecnica di oscuramento.

Tutti gli accessi al sistema di videosorveglianza da parte delle Forze di Polizia saranno documentati mediante l’annotazione in un apposito *“registro degli accessi”* (cartaceo od informatico), conservato nei locali della Centrale Operativa della Polizia Locale, nel quale sono riportati ad opera degli incaricati: la data e l’ora dell’accesso, l’identificazione del terzo autorizzato, i dati per i quali si è svolto l’accesso, gli estremi e la motivazione dell’autorizzazione all’accesso; le eventuali osservazioni dell’incaricato; la sottoscrizione del medesimo e verrà redatto verbale di consegna.

Copia delle immagini e filmati integrali potranno essere rilasciate solo ed esclusivamente all’Autorità Giudiziaria ed alle Forze di Polizia per finalità di polizia giudiziaria e accertamenti amministrativi.

A seguito di segnalazione e/o denuncia di fatti rilevanti dal punto di vista penale, il Comando Polizia Locale provvederà ad estrapolare le immagini e a trattarle per le finalità delle indagini. Tali immagini, che contengono anche altri dati personali e/o particolari, non potranno mai essere consegnate integralmente al segnalante e/o denunciante salvo specifica autorizzazione dell’Autorità Giudiziaria, secondo la normativa di settore.

5. Possono essere divulgate immagini provenienti dagli impianti di videosorveglianza solo previa anonimizzazione di ogni dato che consenta l’identificazione dei soggetti ripresi e solo se autorizzati dal Dirigente della Polizia Locale.

Art. 24 - Sicurezza dei dati

I dati personali oggetto di trattamento sono conservati presso la centrale di registrazione individuata, alla quale può accedere il solo personale autorizzato secondo istruzioni che vengono impartite dal designato al trattamento dei dati.

In ogni caso, gli autorizzati sono istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento.

Il Titolare adotta le misure di sicurezza organizzative, logiche e informatiche al fine di garantire la sicurezza dei dati contro rischi di perdita di riservatezza, disponibilità ed integrità.

Art. 25 – Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

Per quanto attiene al profilo di tutela amministrativa o giurisdizionale si rinvia integralmente a quanto disposto dalle norme in materia di accesso ai documenti amministrativi e a quanto disposto dagli artt. 77 e ss, GDPR ed agli artt. 37 e seguenti del D. Lgs. 51/2018.

Art. 26 - Cessazione del trattamento dei dati

In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti o conservati secondo quanto previsto dall'art. 5 lett. d) GDPR ovvero dall'art 3 della D.Lgs 51/2018 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Art. 27 – Comunicazione e pubblicità

Copia del presente Regolamento, a norma dell'art. 22, Legge 7 agosto 1990, n. 241 e ss.mm.ii., sarà tenuta a disposizione del pubblico perché ne possa prendere visione in qualsiasi momento.

Copia dello stesso sarà altresì pubblicata sul sito internet istituzionale del Comune di Oristano ai fini di pubblicità legale.

Art. 28 - Modifiche regolamentari

I contenuti del presente Regolamento dovranno essere aggiornati nei casi di revisione normativa in materia di trattamento dei dati personali e in materia di videosorveglianza da parte del Consiglio Comunale, o nei casi di miglioramenti tecnologici allo stato non previsti, che comportino la modifica del presente regolamento.

CAPO V

DISPOSIZIONI FINALI

Art. 29 - Rinvio

Per tutto quanto non espressamente disciplinato dal presente Regolamento, si fa rinvio alla Legge, ai suoi provvedimenti di attuazione, alle decisioni del Garante, alle disposizioni del RGPD e D. Lgs.

10 agosto 2018, n. 101, e ad ogni altra normativa vigente, speciale, generale, nazionale e comunitaria in materia.

Art. 30 - Entrata in vigore e disposizioni collegate

Il presente Regolamento, dopo l'esecutività della deliberazione del Consiglio Comunale che lo approva, è pubblicato per quindici giorni all'Albo pretorio *on line* ed entra in vigore il giorno della pubblicazione; conseguentemente, con la medesima deliberazione del Consiglio Comunale si abroga il precedente regolamento per la videosorveglianza in Città approvato con deliberazione C.C. n. 63 del 10 settembre 2019.