Comune di

ORISTANO

REGOLAMENTO
PER LA DISCIPLINA DELLA
VIDEOSORVEGLIANZA

Approvato con Delibera del Consiglio Comunale n.63 del 10 settembre 2019

INDICE

ALLEGATI

Regolamento UE n. 2016/679 del 27 aprile 2016

Premessa

1)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.
2)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.
- *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

1) Il presente regolamento ha per oggetto la disciplina delle misure procedimentali 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.

2) 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

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

2) 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;

3) 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

1) Ai fini del presente regolamento si intende:

a) Per "**banca di dati**", il complesso di dati personali, formatosi presso la sala operativa/di controllo, e trattato esclusivamente mediante riprese video che, in relazione ai luoghi di installazione delle videocamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;
b) Per il "**trattamento**", tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, l'elaborazione, la

modificazione, la selezione, la consultazione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, la limitazione, il blocco, la comunicazione, mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, la cancellazione e la distribuzione di dati;

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**", la cui si riferiscono i dati personali;
j) Per "**consenso dell'interessato**", qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
k) Per "**violazione dei dati personali",** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
l) Per "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
m) Per "**diffusion**e", il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
n) Per "**dato anonimo**", il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile,
o) Per "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
p) 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;

q) 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;
r) 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

1) Il trattamento dei dati personali è effettuato a seguito dell'attivazione del sistema di videosorveglianza nel territorio del Comune di Oristano.

2) 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.

3) 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 tramite:

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) Attivazione di 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;
a) 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;
b) Sorveglianza di particolari aree e siti ad alto rischio di alterazione degli equilibri ambientali;
c) 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 eventualmente amministrativa;
d) 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;
e) Rilevamento di situazioni di occupazione abusiva del suolo pubblico e di disturbo alla quiete pubblica;
f) Acquisire prove pertinenti e rilevanti, idonee a dimostrare l'esistenza del fatto storico da provare;
g) 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

1) Il sistema consiste di una Centrale Operativa, con funzioni di controllo e supervisione, collocata presso il Comando Polizia Locale, di *servers* per la registrazione delle immagini collocato presso i locali del Comando P.L. e da un insieme di punti di ripresa costituiti da telecamere fisse e/o brandeggiabili dislocate nel territorio comunale.

2) Le immagini videoriprese dalle telecamere sono trasmesse alla Centrale Operativa tramite un'infrastruttura di rete geografica di tipo proprietario, dedicato esclusivamente a tale servizio, in fibra ottica e/o *wireless*, con trasmissione di tipo digitale ed *encription* dei dati.

Il sistema non è collegato ad altri sistemi né ad alcuna rete pubblica di telecomunicazioni. Non è quindi accessibile da altre periferiche oltre alla Centrale Operativa.

3) La diretta visualizzazione 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 ED ADEMPIMENTI

Art. 6 – Titolare/contitolari del trattamento

1) Il Comune di Oristano, rappresentato ai fini previsti dal RGPD dal Sindaco *pro tempore*, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco, ai sensi dell'art. 2-*quaterdecies* D. Lgs. 10 agosto 2018, n. 101, può delegare le relative funzioni al Dirigente/Responsabile in possesso di adeguate competenze.

2) Il Titolare è tenuto al rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD, già citati all'art. 2, c. 2 del presente.

3) 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 RGPD, 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), di bilancio e di Piano Esecutivo di Gestione, 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.

4) Il Titolare adotta misure appropriate 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;

5) 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 RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.
6) Il Titolare, inoltre, provvede a:

a) Designare i Delegati del trattamento nelle persone dei Dirigenti/Responsabili e dei Funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;
b) Nominare il Responsabile della protezione dei dati;
c) 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;

7) 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.
8) Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.
9) 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.

Art. 7 - Delegati al trattamento

1) Un Dirigente/Responsabile o più Dirigenti/Responsabile del Comune di Oristano, o un Dirigente/Responsabili o più Dirigenti/Responsabili di altro soggetto/Ente, è nominato Delegato al trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Delegato unico 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.
2) 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.
3) 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.
4) 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.
5) 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.
II 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.
6) II 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.
7) II 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 (RPD), 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;

8) 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
1) Il 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.
2) La gestione dell'impianto di videosorveglianza è riservata al personale appartenente all'Ente.
3) 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.
4) Fra coloro che rivestono la qualifica di incaricati, con l'atto di nomina verranno individuati i soggetti cui è affidata la custodia e conservazione delle *password* e delle chiavi di accesso alla sala operativa.

5) L'accesso ai sistemi è consentito esclusivamente al delegato e ai preposti, come indicati nei punti precedenti.

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

1) I monitor degli impianti di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate. L'accesso alla sala di controllo è consentito solamente al personale dell'Ente, autorizzato per iscritto, dal Delegato al trattamento ed agli incaricati addetti ai servizi di polizia locale, di cui ai successivi articoli.

2) Eventuali accessi di persone diverse da quelle appena indicate devono essere autorizzati, dal Delegato al trattamento.

3) Possono essere autorizzati all'accesso:

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 servizi d'istituto;
c) il personale deputato agli interventi di manutenzione;
d) il personale addetto alla pulizia dei locali;

4) Il Delegato della gestione e del trattamento impartisce idonee istruzioni mirate ad evitare acquisizione illecita o rilevamento di dati, da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.

5) Gli incaricati dei servizi di cui al presente regolamento vigilano sul puntuale rispetto delle istruzioni e sulla corretta acquisizione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art. 10 - Obblighi degli operatori

1) 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.

2) 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.

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

Art. 11 – Responsabile alla protezione dati

1) II Responsabile alla protezione dei dati, in seguito indicato con "RPD", può essere individuato nella figura del dipendente di ruolo del Comune, se 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 Delegato del trattamento provvedono affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione. Nel caso in cui il RPD 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 RPD sono indicati in apposito contratto di servizi. II RPD 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,

2) Il Titolare ed il Delegato al trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali,
3) Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
4) Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - od al Responsabile del trattamento.
5) Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art. 12 – Obblighi di notifica
1) Il Comune di Oristano, quale di 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
1) 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 e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi, esatti 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;
e) Trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, con modalità volta a salvaguardare l'anonimato ed in ogni caso successivamente alla fase della raccolta, atteso che le immagini registrate possono contenere dati di carattere personale;

2) 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.
3) 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.
4) Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato.

5) 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 va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. 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.
6) 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, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Art. 14 – Caratteristiche dei sistemi di videosorveglianza
Il sistema consiste di una Centrale Operativa, con funzioni di controllo e supervisione, collocata presso il Comando Polizia Locale, di una sala server attrezzata per la registrazione delle immagini collocato in ambiente protetto da dispositivi di sicurezza situata presso una sede comunale e da un insieme di punti di ripresa costituiti da telecamere fisse e/o brandeggiabili.
Le immagini video riprese dalle telecamere sono trasmesse in diretta alla Centrale Operativa e di Videosorveglianza tramite diverse tipologie di infrastrutture di rete dedicate allo scopo in fibra ottica, wireless e cloud dedicato esclusivamente a tale servizio, con trasmissione di tipo digitale ed *encription* dei dati.
MAN: Per facilitare l'interconnessione dei sistemi di videosorveglianza viene utilizzata, oltre che la rete in fibra 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 d altissimo livello di sicurezza a norma del RGPD.
RTR: una parte del sistema di videosorveglianza, sarà 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 è 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.
La RAS per poter comunicare, interagire e gestire l'hardware di sorveglianza associato al progetto, attraverso il proprio *DVMS* (*Digital Video Management System)*, si 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 di tutte le telecamere, brandeggiare (in orizzontale ed in verticale) e zoomare gli obbiettivi delle telecamere.

In caso di necessità sarà anche possibile visualizzare le registrazioni delle telecamere stesse.
Di seguito vengono indicate le tipologie di infrastrutture di rete dedicate:

a) VIDEOSORVEGLIANZA PARTECIPATA

Nell'ambito di programmi di sicurezza partecipata e di recupero della cultura della legalità, l'esigenza di sicurezza viene affrontata nella convinzione che una strategia efficace, capace di far fronte realmente alla crescente e pressante domanda di sicurezza, sia quella che promuova un approccio multidisciplinare e integrato, all'interno del quale, gli strumenti penali, cui viene riservato il ruolo di "estrema ratio", vengano affiancati da una vasta gamma di interventi preventivi da cui traspare la dimensione plurale e relazionale del concetto di sicurezza frutto della collaborazione tra istituzioni e cittadini.
La "videosorveglianza integrata", in tal senso, può essere declinata nella ricerca di nuove forme di cooperazione con il cittadino contro quell'ampio spettro di fenomeni che ne turbino la tranquillità, sia che abbiano natura criminale, sia che attengano a quei comportamenti-atti di inciviltà, che limitano il libero utilizzo degli spazi pubblici o che rendono pericoloso il contesto sociale.
Tale sistema di videosorveglianza può dare una possibile risposta e contribuire ad innalzare le attuali aspettative in termini di sicurezza o di vivere la Città "in sicurezza", come da disposto di cui alla Legge 18 aprile 2017, n. 48, sulle «Disposizioni urgenti in materia di sicurezza delle città.», art. 7 "Ulteriori strumenti e obiettivi per l'attuazione di iniziative congiunte", che consente anche la partecipazione di soggetti privati.

b) VIDEOSORVEGLIANZA IN CLOUD

Il sistema di videosorveglianza in *Cloud* è un sistema che consente la gestione e il controllo di telecamere IP e la registrazione di quanto riprendono direttamente, tramite internet, su uno spazio server remoto.
Le telecamere si collegano al *cloud*, situato su un Data Center che raccoglie i dati delle registrazioni delle telecamere in un ambiente sicuro e protetto con protocolli di rete crittografati, attraverso *routers e* utilizzando una connessione Internet a banda larga, ADSL via cavo, INTERNET FIBRA e ne trasferisce, in modalità cifrata certificata, il flusso video direttamente presso la Centrale Operativa della Polizia Locale sia nel caso di telecamere di proprietà comunale e o altri enti, sia di soggetti privati, favorendo la partecipazione di più soggetti e quindi alla Videosorveglianza Partecipata, come descritto al precedente punto a);

Art. 15 - Sicurezza del trattamento

1) Il Comune di Oristano, e ciascun Delegato al trattamento mettono in atto misure tecniche ed organizzative adeguate per 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.
2) 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,
3) 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;

4) 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,

5) 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.

6) 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.*

7) 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

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

2) 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.

3) La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato.

Nel caso in cui un trattamento soddisfi almeno due dei criteri di cui all'art. 35, p. 3 sopra citato, occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4) II Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa; lo stesso può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune. II Titolare deve consultarsi con il RPD 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. II RPD monitora lo svolgimento della DPIA. II Delegato al trattamento deve assistere il Titolare nella conduzione 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.

5) II RPD 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.
6) La DPIA non è necessaria nei casi in cui il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1 RGDP.

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

1) 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 organi competenti.
2) 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, e Polizia Locale e l'Autorità Giudiziaria.
3) L'apparato di videosorveglianza potrà essere utilizzato anche in relazione ad indagini delegate dall'Autorità Giudiziaria.
4) 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 – Il rilievo penale del deposito incontrollato dei rifiuti

In relazione alla incontrollobilità 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.).
1) 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 l'utilizzo non autorizzato di aree impiegate come discariche di materiali e di sostanze pericolose.
2) Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, Legge 24 novembre 1981, n. 689 e ss.mm.ii.).
3) 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

1) Per violazione dei dati personali, in seguito "*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.
2) II 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. II Delegato al trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3) La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

4) 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

1) In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, 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 20 giorni dalla data di ricezione della richiesta, ovvero di 20 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.

2) 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.
3) 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.
4) 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.
5) 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.
6) Nel caso di esito negativo all'istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Art. 21 – Sistemi mobili

1) Il sistema di videosorveglianza mobile è per sua natura composto da apparati trasportabili, e 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, verrà effettuato il controllo dei siti di interesse.

CAPO IV

DELLE TUTELE E DELLE MODIFICHE

Art. 22 – Informative e livelli essenziali di tutela

1) Il Comune di Oristano in prossimità o nelle immediate vicinanze, non necessariamente a contatto con le telecamere, 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*".

2) La registrazione è effettuata dal Comune per fini di prevenzione e sicurezza [Regolamento Europeo sulla protezione dei dati personali RGDP 2016/679 e Provvedimento del Garante per la protezione dei dati personali in materi di videosorveglianza 8 aprile 2010 (G.U. N. 99, del 29/04/2010)].

Tale segnaletica con l'informativa deve avere un formato ed un posizionamento chiaramente visibile.

Art. 23 – Esercizio dei diritti dell'interessato

1) Tutti gli accessi alla visione 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.

2) Non possono, di norma, essere rilasciate copie delle immagini registrate concernenti altri soggetti diversi dall'interessato, salvi casi particolarmente meritevoli di tutela a giudizio insindacabile del Titolare; se le immagini contengono dati riferibili a terzi, l'accesso del richiedente è consentito soltanto se la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi a terzi. Copia delle immagini potranno essere rilasciate solo ed esclusivamente all'Autorità Giudiziaria ed alle Forze di Polizia per finalità di indagini giudiziarie, amministrative e risarcimento danni.

3) A seguito di segnalazione e/o denuncia di fatti rilevanti da un punto di vista giudiziario, amministrativo e risarcitorio il Comando Polizia Locale provvederà ad estrapolare le immagini e a trattarle per le finalità delle indagini di polizia. Tali immagini, che riproducono anche altri dati personali e/o particolari, non potranno mai essere consegnate al segnalante e/o denunciante salvo specifica autorizzazione del Garante della Privacy e dell'Autorità Giudiziaria.

Art. 24 – Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

1) Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, RGPD ed al D. Lgs. 10 agosto 2018, n. 101.

Art. 25 – Comunicazione e pubblicità

1) Non si considera comunicazione, ai sensi e per gli effetti del precedente articolo, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal delegato e che operano sotto la loro diretta autorità.

2) 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.

3) Copia dello stesso sarà altresì pubblicata sul sito internet istituzionale del Comune di Oristano ai fini di pubblicità legale.
4) Copia del presente Regolamento dovrà essere depositato presso la sede del Comune di Oristano a cura del Titolare, a disposizione del Garante per la Protezione dei Dati Personali.

Art. 26 - Cessazione del trattamento dei dati

1) In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:
   a) Distrutti;
   b) Ceduti ad altro titolare purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
   c) Conservati per fini esclusivamente istituzionali dell'impianto attivato.

2) La cessione dei dati in violazione di quanto previsto dal comma precedente lett. b) o di altre disposizioni di legge in materia di trattamento dei dati personali è priva di effetti. Sono fatte salve le sanzioni previste dalla legge.

Art. 27 - Modifiche regolamentari

1) 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

DELLE DISPOSIZIONI FINALI

Art. 28 - Rinvio

1) 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. 29 - Entrata in vigore e disposizioni collegate

1Il 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 successivo all'ultima pubblicazione; conseguentemente, con la medesima deliberazione del Consiglio Comunale n.63 del , si abroga il precedente regolamento per la videosorveglianza in Città approvato con deliberazione C.C. n. 15 del 02/03/2011.

Allegato: Regolamento UU n. 201/679 del 27 aprile 2016