Comune di Ittireddu

Comune di Ittireddu

REGOLAMENTO
PER LA DISCIPLINA DELLA
VIDEOSORVEGLIANZA

Approvato con deliberazione del Consiglio Comunale n. 6 in data 26 febbraio 2020

INDICE

CAPO I
PRINCIPI GENERALI

Articolo 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, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.
2) Il presente regolamento garantisce altresì i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento di dati.
3) Il presente Regolamento 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.

Articolo 2 - Ambito di applicazione
1) Il presente regolamento disciplina il trattamento dei dati personali, realizzato mediante sistema di videosorveglianza, attivato nel territorio del Comune di Ittireddu.
2) L'utilizzo del sistema della videosorveglianza viene attuato attraverso un corretto impiego delle applicazioni e nel rispetto dei principi di cui all'art. 5, del Regolamento UE Generale sulla protezione dei dati personali 2016/679, di seguito RGDP:

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, leciti ed espliciti.
f) **Necessità**, con esclusione di uso superfluo della videosorveglianza.

Articolo 3 – Definizioni
1) Ai fini del presente regolamento si intende:

a) Per "**banca di dati**", il complesso di dati personali, formatosi presso la sala 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, persona giuridica, Ente o associazione, identificata o identificabile ("interessato"). Si considera

identificabile la persona fisica, persona giuridica, Ente o associazione, 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**", l'Ente Comune di Ittireddu, 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 tratti 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 responsabile del trattamento.
i) Per "**interessato**", la persona fisica o giuridica, l'Ente o associazione 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 "**immagin**e", 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 31.1.1996 n. 675, di controllo indipendente per la protezione dei dati personali art. 14, comma 1, lett. b) D.Lgs. 10 agosto 2018, n. 101.

Articolo 4 – Finalità del trattamento dei dati personali per attività di videosorveglianza

1) Il trattamento dei dati personali è effettuato a seguito dell'attivazione del sistema di videosorveglianza nel territorio del Comune di Ittireddu.
2) Presso la sede operativa del Comune, secondo quanto disciplinato dal presente regolamento, sono posizionati monitor per la visualizzazione delle immagini riprese dalle telecamere.
3) Il trattamento dei dati, effettuato mediante l'attività di videosorveglianza, è realizzato nel rispetto delle seguenti disposizioni normative:

a) Art. 615-bis del Regio Decreto 19 ottobre 1930, n. 1398 successive modifiche 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.
b) Legge 20 maggio 1970, n. 300.
c) Legge 7 marzo 1986 n. 65.
d) D.Lgs. 31 marzo 1998, n. 112.
e) D.Lgs. 18 agosto 2000, n. 267.
f) D.Lgs. 30 giugno 2003, n. 196 e relative modifiche D.lgs. 14 marzo 2013, n. 33.
g) Circolare del Ministero dell'Interno n° 558/A/421.2/70/456, del 08.02.2005.
h) L. R. Sardegna 02 agosto 2007, n. 9.
i) Legge 24 luglio 2008, n. 125, di conversione, con modifiche, del D. L. 23 maggio 2008, n. 92.
j) D.M. Interno 5 agosto 2008 (G.U. N. 186, del 09/08/2008)
k) Legge. 23 aprile 2009, n. 38, di conversione, con modifiche del D.L. 23 febbraio 2009, n. 11.
l) Provvedimento del Garante per la protezione dei dati personali in materi di videosorveglianza 8 aprile 2010 (G.U. N. 99, del 29/04/2010)
m) Circolare del Ministero dell'Interno n° 558/A421.2/70/195860, del 06.08.2010.
n) Circolare del Ministero dell'Interno n° 558/SICPART/421.2/70/224632 del 02.03.2012.
o) 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.
p) 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.
q) Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia".
r) D.Lgs.10 agosto 2018, n. 101.
s) Statuto Comunale.
t) Regolamenti Comunali vigenti.

4) Il trattamento dei dati è conforme alle finalità istituzionali demandate al Comune di Ittireddu, ed in particolare sul territorio comunale, attraverso l'acquisizione in tempo reale di dati ed immagini, si intende:

a) Attivare uno strumento operativo di Protezione Civile.
b) Monitorare gli snodi stradali di maggiore rilevanza interessanti la comunità locale, al fine di prevenire i problemi inerenti i flussi veicolari e la mobilità stradale, vigilando sul pubblico traffico ed identificando situazioni di rischio, per consentire il pronto intervento degli organi di polizia.
c) Accertare situazioni di pericolo per la sicurezza urbana connessa alla circolazione stradale, rilevando nelle situazioni di estremo pericolo per gli utenti della strada infrazioni al Codice della Strada derivanti da comportamento di guida quali, il mancato rispetto delle direzioni obbligatorie, dei sensi unici, della circolazione contromano, dei divieti di sosta, all'occupazione di corsie riservate alla circolazione pedonale, dell'omissione di soccorso in caso di incidente stradale, più complessivamente il mancato rispetto delle norme di comportamento in grado di pregiudicare la sicurezza stradale, ciò consentendo in casi di estremo pericolo l'intervento degli operatori.
d) Sorvegliare determinate aree e siti ad alto rischio ambientale al fine di garantire un elevato grado di sostenibilità delle zone monitorate.

e) Controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di area impiegata come discarica di materiali e sostanze pericolose.
f) Tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e prevenire eventuali atti di vandalismo o danneggiamento del patrimonio pubblico.
g) Rilevare situazioni di occupazione abusiva del suolo pubblico e di disturbo alla quiete pubblica.
h) Prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi assicurare maggiore sicurezza ai cittadini.
i) Salvaguardare l'incolumità degli individui ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e sicurezza pubblica, favorendo la protezione delle fasce più deboli della popolazione, garantendo quindi un certo grado di sicurezza negli ambienti circostanti gli edifici comunali, le piazze, le scuole, i parchi, parcheggi, complessivamente della proprietà pubblica e privata soggetta al pubblico utilizzo, accertando e reprimendo i reati per una migliore razionalizzazione dei servizi offerti all'utenza, al fine di farne accrescere la sicurezza, nel pieno rispetto delle competenze attribuite dalla legge all'ente locale Comune.
j) Acquisire prove pertinenti e rilevanti, idonee a dimostrare l'esistenza del fatto storico da provare.

5) 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.

Articolo 5 – Condizioni per il consenso al trattamento

1) Il trattamento dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni che sono assoggettate ad un regime di tipo particolare.
2) Il trattamento dei dati personali nell'ambito di cui trattasi è ordinato all'ambito di applicazione disciplinato dall'articolo 2 del presente regolamento.
3) In relazione ai principi di pertinenza e di 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.

Articolo 6 – Diretta visione delle immagini

1) Il sistema di videosorveglianza deve essere realizzato nella piena compatibilità con le tecnologie analoghe a quelle adottate nelle sale/centrali operative delle forze di polizia ed in quanto tale in grado di garantire i servizi di monitoraggio ed il conseguente, eventuale, allertamento della sala o centrale operativa delle forze di polizia a livello statale, regionale e locale.
2) La diretta visualizzazione delle immagini rilevate con i sistemi di videosorveglianza nelle sale o centrali operative è limitata ad obiettivi particolarmente sensibili e strategici per la sicurezza urbana o in presenza del requisito di pubblico interesse nel pieno rispetto dell'ambito di applicazione disciplinato dall'articolo 3 del presente regolamento e di non eccedenza dei dati o dei trattamenti.
3) Il responsabile si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto.

CAPO II
DEL TITOLARE TRATTAMENTO

Articolo 7 - Notificazione

1) Il Comune di Ittireddu, nella sua qualità 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.

2) I dati trattati devono essere notificati al Garante solo se rientrano nei casi specificatamente previsti dalla normativa vigente sulla protezione dei dati personali. A tale proposito 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.

3) La funzione di titolare del trattamento viene svolta dal Sindaco pro tempore quale rappresentante legale dell'Amministrazione Comunale.

Articolo 8 - Titolare del trattamento

1) II Comune di Ittireddu, 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 del D.Lgs. 10 agosto 2018, n. 101, può delegare le relative funzioni ad un dipendente del Comune in possesso di adeguate competenze.

2) II Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD:

a) Liceità.
b) Correttezza e trasparenza.
c) Limitazione della finalità.
d) Minimizzazione dei dati.
e) Esattezza.
f) Limitazione della conservazione.
g) Integrità e riservatezza.

3) II 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 articoli 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'articolo 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato.
b) Le informazioni indicate dall'articolo 14 RGPD, qualora i dati personali non 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'articolo 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 Responsabili del trattamento nelle persone 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) Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'articolo 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
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'articolo 4 dello statuto dei lavoratori (*legge 300 del 20 maggio 1970 e successive modificazioni*), per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

Articolo 9 - Responsabile del trattamento

1) Un funzionario o più funzionari, addetti agli uffici in cui si articola l'organizzazione del Comune di Ittireddu, sono nominati Responsabili unici del trattamento delle banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile 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'articolo 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.
2) Il responsabile o i responsabili del 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 responsabile designato.
3) II 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 comma 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 del trattamento e le modalità di trattamento.
4) Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'articolo 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-responsabile.
6) II Responsabile del 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 Responsabile del 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 ed alla 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 responsabile custodisce le chiavi per l'accesso ai locali della centrale di controllo, le chiavi degli armadi per la conservazione delle videocassette/CD o altro supporto informatico, nonché le parole chiave per l'utilizzo dei sistemi.

Articolo 10 – Nomina degli incaricati e dei preposti alla gestione dell'impianto di videosorveglianza

1) Il responsabile designa e nomina nell'ambito del personale del Comune i preposti in numero sufficiente a garantire la gestione del servizio di videosorveglianza. Incaricherà, comunque, tutti gli operatori che in via principale o residuale effettuano o dovranno effettuare un trattamento dei dati.
2) I preposti andranno nominati tra soggetti, che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
3) La gestione dell'impianto di videosorveglianza è riservata al personale del Comune.
4) Con l'atto di nomina, ai singoli preposti saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.
5) In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento.
6) Nell'ambito degli incaricati, verranno designati, con l'atto di nomina, i soggetti cui è affidata la custodia e conservazione delle password e delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti contenenti le immagini.
7) L'accesso ai sistemi è consentito esclusivamente al responsabile e ai preposti, come indicati nei punti precedenti.
8) I preposti, previa comunicazione scritta al responsabile, potranno autonomamente variare la propria password.

Articolo 11 – Persone autorizzate ad accedere alla sala di controllo

1) L'accesso alla sala di controllo è consentito solamente al personale del Comune e al personale tecnico appositamente incaricato, autorizzato per iscritto, dal Responsabile del trattamento ed agli incaricati addetti ai servizi, di cui ai successivi articoli.
2) Eventuali accessi di persone diverse da quelli innanzi indicate devono essere autorizzati, per iscritto, dal Responsabile del trattamento.
3) Possono essere autorizzati all'accesso solo incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità di cui al presente regolamento, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali e il personale delle forze dell'ordine.
4) Il Responsabile della gestione e del trattamento impartisce idonee istruzioni atte ad evitare assunzioni 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 assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Articolo 12 - 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 articolo, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'articolo 3 comma 2 ed a seguito di regolare autorizzazione di volta in volta richiesta al Responsabile del trattamento dei dati personali designato.
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.

Articolo 13 - Responsabile della protezione dati
1) II Responsabile della protezione dei dati, in seguito indicato con "RPD", può essere individuato nella figura del dipendente di ruolo del Comune o del soggetto/Ente convenzionato. L'RPD può essere scelto fra i dipendenti del Comune purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il Titolare ed il Responsabile 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 mediante procedura ad evidenza pubblica 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 Responsabile del trattamento.
Nel caso di Comuni di servizi che svolgono il servizio in forma associata, è possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più comuni mediante esercizio associato della funzione nelle forme previste dal D. Lgs. 18 agosto 2000 n. 267.
II RPD è incaricato dei seguenti compiti:

a) Informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al

Responsabile del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato.

b) Sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento.
c) Sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento.
d) Fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD.
e) Cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare o dal Responsabile del trattamento al Garante.
f) La tenuta dei registri di cui ai successivi articoli 16 e 17.
g) Altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi.

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

2) Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, a tal fine:

a) Il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili di P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali.
b) Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale.
c) Il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione.
d) Il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

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. In tal senso il RPD:

a) Procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati.
b) Definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

4) Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

5) La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili (in relazione alle dimensioni organizzative del Comune):

a) Il Responsabile per la prevenzione della corruzione e per la trasparenza.
b) Il Responsabile del trattamento.
c) Qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

6) II Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

a) Supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e della Giunta Comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance.
b) Tempo sufficiente per l'espletamento dei compiti affidati al RPD.
c) Supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero (in relazione alle dimensioni organizzative dell'Ente) tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale).
d) Comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente.
e) Accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

7) II RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.
8) II RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.
9) Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - od al Responsabile del trattamento.
10) 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.

CAPO III
DEL TRATTAMENTO DEI DATI PERSONALI

Articolo 14 - Modalità di 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 precedente articolo 4 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 comma 4.
e) Trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, di cui al precedente articolo 4 comma 4, lett. b), 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 telecontrollo e di videosorveglianza, installate in corrispondenza di intersezioni, piazze, parchi pubblici e immobili, del territorio urbano. Detta procedura verrà seguita anche in caso di modifiche e/o integrazioni di detto elenco.

3) Le telecamere di cui al precedente comma 2 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

I segnali video delle unità di ripresa saranno raccolti da una stazione di monitoraggio e controllo presso la sala controllo del soggetto convenzionato. Le immagini saranno visualizzate su monitor e registrate su un supporto digitale. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento.

5) Le attività di videosorveglianza sono finalizzate alla tutela della sicurezza urbana e alla luce delle recenti disposizioni normative, il termine massimo di durata della conservazione dei dati è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di video sorveglianza, fatte salve speciali esigenze di ulteriore conservazione. In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante, e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. 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 dovrà essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Articolo 15 - Sicurezza del trattamento

1) Il Comune di Ittireddu, e ciascun Responsabile del 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, 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 Responsabile del 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 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 Ittireddu, e ciascun Responsabile del trattamento 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, del o dei Responsabili del trattamento e del Responsabile della 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.

Articolo 16 - Registro delle attività di trattamento

1) Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) Il nome ed i dati di contatto del Comune, del Sindaco e/o del suo Delegato, eventualmente del contitolare del trattamento, del RPD.
b) Le finalità del trattamento.
c) La sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali.
d) Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati.
e) L'eventuale trasferimento di dati personali verso un Paese Terzo od una organizzazione internazionale.
f) Ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati.
g) Il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente articolo 15.

2) Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato, presso gli uffici della struttura organizzativa del soggetto/Ente convenzionato, in forma telematica/cartacea. Nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente comunale.

3) Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

4) In relazione alle dimensioni organizzative del Comune, il Titolare può decidere di tenere un Registro unico dei trattamenti che contiene le informazioni di cui ai commi precedenti e quelle di cui al successivo articolo17, sostituendo entrambe le tipologie di registro dagli stessi disciplinati. In tal caso, il Titolare delega la sua tenuta al Responsabile unico del trattamento, comunque, ad un solo Responsabile del trattamento, ovvero può decidere di affidare tale compito al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Articolo 17 - Registro delle categorie di attività trattate

1) Il Registro delle categorie di attività trattate da ciascun Responsabile reca le seguenti informazioni:
   a) Il nome ed i dati di contatto del Responsabile del trattamento e del RPD.
   b) Le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali.
   c) L'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale.
   d) Il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente articolo 15.

2) Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea.

3) II Responsabile del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.

Articolo 18 - 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, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'articolo 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. 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'articolo 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'articolo 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.
   b) Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche.
   c) Monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico.
   d) Trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'articolo 9 RGDP.
   e) Trattamenti di dati su larga scala, tenendo conto dei soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento.
   f) Combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato.
   g) Dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio

nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori.

h) Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative.
i) Tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati 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. Il Titolare 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 Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile 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 io 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.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o 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 seguenti:

Se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'articolo 35, p. 1 RGDP:

a) Se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento.
b) Se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche.
c) Se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7) La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) Descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei).
b) Valutazione della necessità e proporzionalità dei trattamenti, sulla base:
    I. Delle finalità specifiche, esplicite e legittime.
    II. Della liceità del trattamento.
    III. Dei dati adeguati, pertinenti e limitati a quanto necessario.
    IV. Del periodo limitato di conservazione.

V. Delle informazioni fornite agli interessati.
VI. Del diritto di accesso e portabilità dei dati.
VII. Del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento.
VIII. Dei rapporti con i responsabili del trattamento.
IX. Delle garanzie per i trasferimenti internazionali di dati.
X. Consultazione preventiva del Garante del trattamento dei dati personali.

c) Valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati.
d) Individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8) II Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
9) Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA Condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.
10) La DPIA deve essere effettuata, con eventuale riesame delle valutazioni condotte, anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Articolo 19 -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 Responsabile della videosorveglianza provvederà a darne immediata comunicazione agli organi competenti.
2) In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa di cui al precedente articolo 14, 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, della Polizia Regionale o 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, della Polizia Regionale o Polizia Locale, 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 Responsabile della gestione e del trattamento dei dati.

Articolo 20 - Il deposito dei rifiuti

1) In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta consentito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.
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, l. 24 novembre1981, n. 689).

Articolo 21 - Violazione dei dati personali

1) Per violazione dei dati personali, in seguito "data breach", si 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 Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3) I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando articolo 75 RGPD, sono i seguenti:

a) Danni fisici, materiali o immateriali alle persone fisiche.
b) Perdita del controllo dei dati personali.
c) Limitazione dei diritti, discriminazione.
d) Furto o usurpazione d'identità.
e) Perdite finanziarie, danno economico o sociale.
f) Decifratura non autorizzata della pseudonimizzazione.
g) Pregiudizio alla reputazione.
h) Perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4) Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

a) Coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati.
b) Riguardare categorie particolari di dati personali.
c) Comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze).
d) Comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito).
e) Impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

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

6) 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 ei 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.

Articolo 22 - 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 responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati.

c) Di ottenere, a cura del Responsabile, senza ritardo e comunque non oltre venti giorni dalla data di ricezione della richiesta, ovvero di venti 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 comma 1, lett. c), n. 1), 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 comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.
5) Le istanze di cui al presente articolo possono essere trasmesse al titolare o al soggetto convenzionato, nominato responsabile, mediante lettera ordinaria o raccomandata, posta elettronica o posta certificata, che dovrà provvedere in merito entro e non oltre trenta giorni.
6) Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.
7) Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.
La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.
In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo; viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge.

Articolo 23 - Sistemi integrati di videosorveglianza
1) Nell'ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

a) Gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti

istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati.

b) Collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'articolo 29 del Codice da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare.
c) Sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia. L'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia - individuato ai sensi dell'articolo 13, comma 3, del Codice e riportato in fac-simile nell'allegato n. 2 al citato provvedimento del Garante. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati.

3) Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle individuate nel precedente punto 3.3.1 del citato provvedimento del Garante, quali:

a) Adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi.
b) Separazione logica delle immagini registrate dai diversi titolari.

4) Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare al Garante.

Articolo 24 - Sistemi integrati di videosorveglianza enti pubblici e territoriali, altre cautele

1) Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, alfine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.

2) È stato individuato al punto 4.6 del citato provvedimento del Garante un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale. In particolare:

a) L'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente.
b) Nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.

3) Il titolare del trattamento è tenuto a richiedere una verifica preliminare al Garante fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di

videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già il punto 3.2.1 del citato provvedimento del Garante la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

Articolo 25 - Istituti scolastici

1) Il sistema di videosorveglianza attivo presso istituti scolastici dovrà garantire il diritto dello studente alla riservatezza (articolo 2, comma 2, D.P.R. n. 249/1998), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione e al loro diritto all'educazione.
2) In tale quadro, potrà risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti.
3) È vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola.
4) Laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio.

CAPO IV
DELLE TUTELE E DELLE MODIFICHE

Articolo 26 – Informativa

1) Il Comune di Ittireddu, 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 Ittireddu - area video sorvegliata".
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. Può inglobare un simbolo ed eventualmente comunicare se le immagini sono solo visionate o anche registrate.
2) Il Comune di Ittireddu si obbliga a comunicare mediante informativa secondo lo schema MODELLO 1 allegato al presente Regolamento l'avvio del trattamento dei dati personali con la attivazione del sistema di video sorveglianza.
3) Il Comune di Ittireddu nell'ambito della trasparenza, del buon andamento e l'imparzialità dei procedimenti amministrativi indica con modelli da definire che verranno appositamente predisposti, le modalità per esercitare l'accesso alle immagini video da parte delle persone che presumono di essere state riprese dal sistema di videosorveglianza.

Art. 27– 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, previsioni che saranno contenute nel Decreto Legislativo di prossima emanazione recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento

dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

Articolo 28– Comunicazione e pubblicità

1) Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal responsabile e che operano sotto la loro diretta autorità.
2) Copia del presente Regolamento, a norma dell'articolo 22 della Legge 7 agosto 1990, n° 241 e successive modificazioni ed integrazioni, 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 Ittireddu.
4) Copia del presente Regolamento dovrà essere depositato presso la sede del Comune di Ittireddu e del soggetto convenzionato, nominato Responsabile, a disposizione del Garante per la Protezione dei Dati Personali.

Articolo 29 - 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.

Articolo 30 -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.
2) Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi conseguenti al presente Regolamento, in particolare la predisposizione dell'elenco dei siti di ripresa e l'aggiornamento in caso di ampliamento, la fissazione degli orari delle registrazioni, nonché la definizione di ogni ulteriore e specifica disposizione ritenuta utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento.

CAPO V
DELLE DISPOSIZIONI FINALI

Articolo 31 - 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.

Articolo 32 - Entrata in vigore

1) Il presente Regolamento entrerà in vigore alla data di avvenuta esecutività della deliberazione di approvazione.

Il cartello “Area Videosorvegliata” verrà predisposto in conformità alla normativa vigente e alle linee guida n. 3/2019 elaborate dal Comitato Europeo per la protezione dei dati - dedicate alla disciplina del trattamento dei dati attraverso apparecchiature di videoripresa.

Il cartello conterrà le informazioni più importanti quali:

- logo stilizzato della telecamera
- identità del titolare del trattamento ovvero del suo rappresentante (art. 27 del GDPR)
- dati di contatto, ove designato, del Responsabile della Protezione dei Dati
- le finalità del trattamento
- le basi giuridiche del trattamento
- un “accenno” ai diritti dell'interessato.

Il cartello verrà posizionato ad una distanza ragionevole dai luoghi monitorati (approssimativamente all'altezza degli occhi), in modo tale che il cittadino possa facilmente riconoscere l'area controllata dalla telecamera prima che entri nella stessa.

Esempio:

Identità del Titolare del trattamento:

Dettagli di contatto del Data Protection Officer (DPO/RPD) ove applicabile:

Finalità del trattamento dati personali nonché fonti normative per l'elaborazione:

Diritti dell'interessato: *Sono i diversi diritti dell'interessato al trattamento nei confronti del Titolare, in particolare il diritto di accesso o cancellazione dei dati personali.*

Per tutti i dettagli su questo servizio di videosorveglianza, inclusi i tuoi diritti, consulta le informazioni complete fornite dal Titolare attraverso le opzioni riportate a sinistra.