COMUNE DI SENIS
Provincia di Oristano

via Vittorio Emanuele, 09080 Senis (OR) Tel.-. 0783/969031 www.comune.senis.or.it - comunesenis@pec.it - .
protocollo@comune.senis.or.it

REGOLAMENTO COMUNALE SULLA

VIDEOSORVEGLIANZA

Approvato con Deliberazione del Consiglio Comunale n. 25 del 08/06/2021

CAPO I
PRINCIPI GENERALI

Art. 1 – Premessa
Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali. La videosorveglianza dà luogo pertanto a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.

Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune di SENIS nel territorio comunale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Art. 2 - Norme di riferimento e principi generali
Il presente regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto di videosorveglianza cittadina, attivato nel territorio del Comune di SENIS.

Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto dal:

- Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito RGPD) relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
- Direttiva UE 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";
- DPR n. 15 del 15/01/2018 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";
- Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);
- Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008);
- Legge n. 38/2009 recante "misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori".
- Linee Guida 3/2019 sul trattamento di dati personali attraverso Videosorveglianza del Comitato Europeo per la Protezione dei dati adottate in data 29/01/2020.

La Videosorveglianza in ambito Comunale si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5, RGDP e, in particolare:

Principio di liceità – Il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ossequio al disposto di cui all'art. 6, Paragrafo 1, lett. e), RGPD. La videosorveglianza comunale pertanto è consentita senza necessità di consenso da parte degli interessati.

Principio di necessità – In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), RGPD, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.

Principio di proporzionalità – La raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento.

Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere.

Principio di finalità – Ai sensi dell'art. 5, Paragrafo 1, lett. b), RGPD, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana che il DM Interno 05/08/2008 definisce come il "*bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale.*"

Art. 3 – Definizioni

Ai fini del presente Regolamento si intende:

- 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;

- per **«trattamento»**, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- per "**banca dati**", il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;
- per **«profilazione»**, qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- per **«pseudonimizzazione»**, il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- per **«titolare del trattamento»**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- per **«autorizzato al trattamento»**, la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del Titolare o del Designato al trattamento;
- per **«designato allo svolgimento di specifici compiti e funzioni connessi al trattamento»,** la persona fisica espressamente designata che, sotto la responsabilità del Titolare e nell'ambito della propria struttura organizzativa, svolge specifici compiti e funzioni connessi al trattamento dei dati personali;
- 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;
- per **«interessato»**, la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
- per **«terzo»**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- 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;
- 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;
- per "**diffusione**", il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- per "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Art. 4 – Finalità istituzionali dei sistemi di videosorveglianza

Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza attengono allo svolgimento delle funzioni istituzionali proprie dell'amministrazione comunale in conformità a quanto previsto dal:

- D. Lgs. 18 agosto 2000, n. 267 – TUEL;
- D.P.R. 24 luglio 1977, n.616;
- D. Lgs. 31 marzo 1998, n. 112;
- Legge 7 marzo 1986, n. 65, sull'ordinamento della Polizia Municipale;
- Legge 24 luglio 2008, n. 125 recante misure urgenti in materia di sicurezza pubblica;
- Legge 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale;
- Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana;
- Circolari del Ministero dell'Interno n.558/A/421.2/70/456 in data 8 febbraio 2005, n. 558/A421.2/70/195860 in data 6 agosto 2010 e n. 558/SICPART/421.2/70/224632 in data 2.3.2012.

Nella richiamata cornice normativa e all'interno del nuovo sistema di lotta alla criminalità che attribuisce ai Comuni un ruolo strategico nel perseguire finalità di tutela della sicurezza pubblica, l'impianto di videosorveglianza del Comune di SENIS, è precipuamente rivolto a garantire la **sicurezza urbana** che, l'art. 1 del Decreto del Ministero dell'Interno del 5 agosto del 2008, testualmente definisce come il "*bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale.*"

La disponibilità tempestiva di immagini presso il Comune costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale sul territorio comunale, in stretto raccordo con le altre forze dell'ordine. L'archivio dei dati registrati costituisce, infatti, per il tempo di conservazione stabilito per legge, un patrimonio informativo per finalità di Polizia Giudiziaria, con eventuale informativa nei confronti dell'Autorità Giudiziaria competente a procedere in caso di rilevata commissione di reati.

In particolare, il sistema di videosorveglianza attivato dall'Amministrazione, è finalizzato a:

a) incrementare la sicurezza urbana e la sicurezza pubblica nonché la percezione delle stesse rilevando situazioni di pericolo e consentendo l'intervento degli operatori;
b) prevenire, accertare e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito

del più ampio concetto di “sicurezza urbana” già richiamato; le informazioni potranno essere condivise con altre forze di Polizia competenti a procedere nei casi di commissione di reati;

c) tutelare gli immobili di proprietà o in gestione dell’Amministrazione Comunale e gli edifici pubblici e a prevenire eventuali atti di vandalismo o danneggiamento;
d) controllare le aree considerate a maggiore rischio per la sicurezza, l’incolumità e l’ordine pubblico;
e) al monitoraggio del traffico;
f) attivare uno strumento operativo di protezione civile sul territorio comunale;
g) ad acquisire elementi probatori in fattispecie di violazioni amministrative o penali;
h) per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l’utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
i) monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
j) verificare l’osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.

Gli impianti di videosorveglianza non potranno essere utilizzati, in base all’art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970) per effettuare controlli sull’attività lavorativa dei dipendenti dell’amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati. Gli impianti di videosorveglianza non potranno altresì essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.

L’attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l’angolo visuale delle riprese, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.

La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi.

La possibilità di avere in tempo reale dati e immagini costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell’ambito delle proprie competenze istituzionali; attraverso tali strumenti si perseguono finalità di tutela della popolazione e del patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.

L’uso dei dati personali nell’ambito definito dal presente Regolamento, non necessita del consenso degli interessati in quanto viene effettuato per l’esecuzione di un compito di interesse pubblico o comunque connesso all’esercizio di pubblici poteri e allo svolgimento di funzioni istituzionali di cui è investito il Comune.

Art. 5 – Caratteristiche tecniche dell'impianto

Presso il Comune sono posizionati i monitor per la visione in diretta delle immagini riprese dalle telecamere e le apparecchiature per la relativa registrazione.

Il sistema è composto da:

 N° 8 _ Ir Camera Ip Eco Savvy Da Esterno Ip66 speed dome con le seguenti caratteristiche minime:

Compatibilità **ONVIF**
Sensore 1/2.8" CMOS
Ottica 5-129 mm (optical zoom)
Illuminazione minima 0.05Lux/F1.4 (color)
0Lux /F1.4 (IR)
IR Si
Massima distanza IR (328ft) 150 Mt.
Compressione video H264 / H264+
Preferibile H265
Risoluzione 3 Mp (2048 x 1536)
Frame rate 30fps@1.3M/720P
Multi-streaming 3 streams
Analisi video Tripwire, intrusion
Abandoned/missing
Face detection
Slot SD card Micro SD
Grado di protezione IP66 o IP67
Temperatura di esercizio -10 / +50

 N° 7 Ir Camera Ip Eco Savvy Da Esterno Ip66 per lettura targhe con le seguenti caratteristiche minime

Compatibilità ONVIF -OCR
Sensore 1/2.8" CMOS
Ottica 3.6mm/F2.0
Illuminazione minima 0,01/F2.0 (color)
0,01 F1.2 (IR)
Day/night ICR
Massima distanza IR 30m
Compressione video H265
Risoluzione 2 Mpixel
Frame rate 50/60fps@10800P
Multi-streaming 2/3 streams
Analisi video Tripwire, intrusion
Scene change
Abandoned/missing

Face detection
Grado di protezione IP66 o IP67
Temperatura di esercizio ~ -30°c ~ +-+ 50 °c

 N° 8 Staffa di fissaggio a parete per box e IR camera con passaggio cavi integrato.
 N° 15 Adattatore da palo o supporto da parete
 N° 8 Alimentatore rain proof switching con ingresso 90~220Vac a morsettiera e uscita stabilizzata a 12Vdc carico massimo 2A, con connettore Jack femmina
 N° 1 NVR di tipo Embedded, sino a 16 ingressi IP. Risoluzione dei canali IP sino a 5Mpixel, banda totale massima in ingresso 160Mbps. Supporta 1 uscita audio, canale voice talk, 1 uscita video HDMI (FullHD), 1 uscita video VGA (FullHD), 1 uscita video CVBS, 4 ingressi allarme, 2 uscite relè, porta RS485 ed RS232. Scheda di rete Ethernet 1Gbps, sino a 128 stream in rete (240Mbps), web server multi-browser, sino a 2HDD SATA da 4TB cadauno, 2 porte USB, alimentatore esterno 12Vdc, consumo 13W, temperatura di esercizio da -10°C a +55°C. --- Saranno installati in Rack presso la postazione di controllo.
 N° 1 Monitor TV led retroilluminato, 40", collegato al computer visualizzerà le telecamere. Possibile collegamento direttamente alla apparecchiatura di Backup.
 SOFTWARE di centralizzazione e gestione da installare su computer , trasmissione delle immagini su monitor TV da 40" gestione delle uscite, possibilità di allarmare in Motion le varie telecamere per una più rapida visualizzazione di un determinato evento
 SOFTWARE OCR compatibile con protocollo Onvif in grado di fornire un flusso Standard RTSP.
 N° 1 Switch Web Managed 20 porte Gigabit + 4 porte Dual Personality Gigabit - Formato Rack 19". La serie GS1910 è ideale per assicurare connettività Gigabit e fornire funzionalità evolute quali ad esempio VLAN e Rapid Spanning Tree. Pronto per le future reti 10 Gigabit Ethernet, lo Switch ZyXEL GS1910 è il prodotto ideale per il collegamento di numerosi dispositivi alimentati a una rete aziendale fornendo una maggiore larghezza di banda verso apparati quali Server o Storage, per alleggerire la congestione e velocizzare la consegna dei dati. Sarà installati in Rack presso la postazione di controllo
 N° 2 Seagate HD 2TB S-ATA III CACHE 64MB. Capacità hard 2.000 GB, dimensione hard disk 88.9 mm (3.5), velocità di rotazione 7200 RPM. Interfaccia hard disk Serial ATA III, dimensioni di buffer 64 MB. Velocità di trasferimento dati 6 Gbit/s. Consumo (tipico) 6.2 W, consumo (stand-by) 4.6 W
 Cavo LAN FTP Categoria 6 schermato doppia guaina matassa da 100 metri o bobine da 500,
 plug RJ45 per le connessioni con protezioni in gomma.
 N° 8 Sistema UPS off-line da 300W / 600VA, backup per 10~20 minuti, 1 batteria da 12V 7AH, protezione LAN e telefono, porta USB per controllo sistema, montaggio a pavimento. Saranno alloggiati nei contenitori in vetroresina contenenti le apparecchiature oppure, se c'è lo spazio necessario, nel contenitore stradale di partenza dell'alimentazione della postazione telecamera.
Un UPS per ogni punto di trasmissione/ripresa video.
 N° 1 UPS 1500/900_ Sistema UPS off-line da 1.500VA / 900W, backup per 3~10 minuti, 2 batterie da 12V 8AH, protezione LAN e telefono, display per controllo sistema, montaggio a rack 19" 2 unità. (Protezione NVR)_ Sarà posizionato nel Rack ed alimenterà il monitor.
 N° 1 UPS3000/2100_ Sistema UPS on-line da 3.000VA / 2.100W, 8 batterie da 12V 7AH, protezione LAN e telefono display per controllo sistema, montaggio a pavimento o rack 19" 2 unità. (Alimentazione linee telecamere) _ Saranno alloggiati nel Rack principale, uno di essi

alimenterà le telecamere ed i ponti di ricezione del sistema WiFi e gli accessori alimentati ad essi connessi; l'altro alimenterà il sistema di backup ed il computer.

 N° 1 Armadio rack serie floor pro 19" 24 unità, L600xP600xH1300, smontato (4 colli), 4 montanti inclusi, verniciatura a polveri epossidiche, grado di protezione ip20, ruote 2,0", piedini regolabili, porta con maniglia a chiave, apertura porta anteriore a 180°, apertura reversibile, spessore lamiera portante 2 mm, spessore lamiera non portante 1,5mm, pannelli laterali e posteriori removibili, ingresso cavi dall'alto e dal basso, capacità di carico 500 kg, colore nero, vetro fumè garanzia standard on-center 12 mesi. Sarà installato in Rack nel locale vigilanza.

 N° 1 Pdu orizzontale 19" in plastica, 1 unità rack, ingresso schuko 16a - 6 uscite Italia 10/16a schuko, lunghezza cavo d'alimentazione 3 mt, sezione conduttori cavo alimentazione 3x1,5 mmq, interruttore luminoso garanzia standard on-center 12 mesi.

 N° 1 Unità ventilante a 2 corpi 1 unita' per rack 19", alimentazione 230vac - 50hz tramite connettori d'ingresso iec320 c14, colore nero garanzia standard on-center 12 mesi

 N° 2 Mensola profondità 250 mm. Con laterali rialzati 1 unità, per rack 19",colore nero garanzia standard on-center 12 mesi.

 N° 8 Fornitura e posa in opera di QUADRO A PORTA CIECA IP65 425x325x180 (hxbxp); telaio componibile e regolabile in profondità; guide DIN regolabili in altezza; pannelli removibili; elevata robustezza; idoneo per installazioni da –25 a +60°; idoneo alla realizzazione di apparecchiature assemblate secondo le Norme EN 61439-1. Chiusura a chiave trilobata o con serratura DIN. Compreso accessori per il fissaggio in modo solidale al palo in VTR. Al suo interno, cablati in ogni parte All'interno di esso troveranno posto:

o N° 1 interruttore magneto termico in classe AC 10 Ah (generale);

o N° 1 interruttore differenziale magneto termico 6 AH classe A contro corto circuiti o correnti differenziali per la protezione della telecamera, a valle vanno collegati:

o Un dispositivo per la protezione contro le sovratensioni (collegamento allo spandente di terra posto ai piedi del palo;

o Un dispositivo di filtraggio per linea di alimentazione per impedire il propagarsi sulla rete d'alimentazione di eventuali disturbi a radiofrequenza;

o Switch di rete barra DIN a 5 porte 10/100Mbps con 4 porte PoE IEEEIEEE802.3°IEEEIEEE802.3at da 15W (max 60W), uscita allarme, alimentazione ridondante 48Vdc massimo 67W, temperatura esercizio -10° ~ +70Uno Switch di rete 5 porte 10/100/1000 Mbps con 4 porte PoE da 15,4 Watt cadauna;

N° 8 Station dotata di antenna a griglia da 23dBi e viene fornita con staffe di montaggio a palo e poe 24V. La tecnologia InnerFeed della Station rappresenta una vera e propria rivoluzione nel mondo del wireless a banda larga, ha un guadagno di 23 dBi grazie al processore Atheros MIPS 24 KC, 400 MHz di cui è provvista. Può essere utilizzata in polarizzazione verticale o orizzontale. E' dotata di un sistema a led per la verifica del livello del segnale e riesce a dare un troughput molto elevato su distanze abbastanza rilevanti. Utilizza il sistema operativo AitOS e protocollo di comunicazione Airmax ed un interfaccia di rete 1x10/100 BASE-TX (Cat. 5, Rj-45).

N° 8 Client/access point a 5Ghz. Si integra perfettamente con le antenne mimo settoriali ed è adatta sia per punti di diffusione che per collegamenti P2P. Ha doppia uscita RPSMA per il collegamento alle antenne, e permette di sfruttare a pieno tutte le potenzialità delle antenne riducendo di moltissimo i problemi di latenza. Il troughput dei dati può arrivare fino a 150Mbps.

Amministrazione web è molto semplice e trasparente e in grado di controllare per esempio questi parametri e funzioni:- Modalità AP, client o WDS - Traffic Shaping - QoS - Routing o bridge trasparente tra la WAN e LAN, con o senza NAT - Potenza del segnale configurabile built-in LED - Potenza di uscita 28 dBi. E' alimentata da alimentazione a 24 V 1A. Il client access include un alimentatore PoE che è dotato di un reset hardware che permette di ripristinare l'apparato, in caso di guasto software, direttamente dal PoE.
N. 2 Antenna omnidirezionale Doppia Polarità 2x2 MIMO che è stata progettata per integrarsi perfettamente con le radio Rocket M . E' sufficiente accoppiare il Rocket M con una Antenna omnidirezionale Doppia Polarità 2x2 MIMO per creare una potente stazione base omnidirezionale 360°. Questa perfetta integrazione offre ai progettisti della rete una impareggiabile flessibilità e convenienza. Nel kit sono inclusi gli accessori per il montaggio del Rocket, gli accessori per il montaggio su palo ed i cavi antenna per esterno. (ricezione client Centro Capena e client Ponte Storto)
N. 8 Antenna parabolica da 400mm: 25 dBi High Performance,
Ideale per CPE wireless client, collegamenti PtP e PtMP a 5 GHz. (trasmissione e ricezione da ponte a zona di controllo)
N° 1 Switch di rete barra DIN a 5 porte 10/100Mbps uscita di allarme per malfunzionamenti, alimentazione ridondante 12~24Vdc massimo 3W, temperatura di esercizio
-10° ~ +70°
L'intervento deve rispondere alla direttiva del Ministero dell'Interno N. 558/SICPART/421.2/70 e deve essere tale da rispettare le specifiche tecniche di interoperabilità ed interfacciamento con la rete telematica regionale (RTR) e digital video management system della Regione Autonoma della Sardegna. L'amministrazione Regionale, ha realizzato un "nodo centralizzato di controllo e di monitoraggio ambientale" veicolato sulla rete telematica regionale, RTR.
Il sistema centralizzato, il cui scopo è il telerilevamento e la supervisione delle reti di sicurezza locale e di monitoraggio ambientale, è in grado di monitorare, visionare, trasferire, in tempo reale, flussi video provenienti dalle reti locali di videosorveglianza dei beneficiari, nel rispetto delle norme sulla privacy e secondo i protocolli di sicurezza, standard tecnologici e disposti per legge e, ove necessario, mediante la stipula di opportune e/o necessarie convenzioni con gli enti preposti alla sicurezza.
Pertanto le reti locali di videosorveglianza devono essere progettate e realizzate in modo che sia garantita tale integrazione e interoperabilità, secondo quanto previsto all'articolo 4, e specificato nei successivi articoli 9, 10 e 11 della convenzione stipulata tra i soggetti beneficiari e la Regione.
La Rete Telematica Regionale (RTR) è 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, IP/MPLS per le sedi periferiche non direttamente interconnesse in fibra ottica e Gigabit Ethernet per le MAN. La RTR adotta il TCP/IP come protocollo standard.
Nelle sedi dove è presente il centro stella delle reti di videosorveglianza locali, sarà attivato un punto di accesso alla RTR. Sarà cura dell'Amministrazione Regionale predisporre un piano di indirizzamento IP armonizzato con quella della RTR. Sarà cura delle Amministrazioni beneficiarie richiedere il proprio piano di indirizzamento prima di iniziare l'installazione degli impianti di

videosorveglianza, al presidio RTR, istituito presso la Direzione generale degli affari generali e società dell'informazione

Per le esigenze e gli scopi descritti nell'Avviso Pubblico e nella convenzione stipulata con gli enti beneficiari, l'amministrazione regionale (RAS), utilizza un sistema di gestione video digitale (DVMS – Digital Video Management System), in grado di inter operare, monitorare gestire i flussi dei sistemi di videosorveglianza locali.

Per garantire l'interoperabilità tra dispositivi, è cruciale l'utilizzo di protocolli standard.

La RAS per poter comunicare, interagire e gestire l'hardware di sorveglianza associato al progetto, attraverso il proprio DVMS, si è dotata, di un software di monitoraggio, in grado di operare con gli eterogenei sistemi di videosorveglianza locali, indipendente da brand e costruttori. Pertanto l'infrastruttura di comunicazione locale dovrà garantire l'apertura delle porte di rete per il transito di tutti i protocolli utilizzati dal DVMS. Dovrà essere garantita la raggiungibilità da parte del DVMS, attraverso la RTR, di tutti gli apparati (videoserver e/o telecamere) grazie al piano di indirizzamento armonizzato citato nel precedente paragrafo

L'amministrazione al fine di garantire la massima interoperabilità e massima compatibilità, ha optato per la scelta del DVMS MILESTONE (VMS Milestone XProtect Corporate Edition) conforme altresì allo standard de facto ONVIF1 e PSIA2, che definiscono una serie di specifiche e accordi tra i produttori sul mercato.

La suddetta interoperabilità si attua concretamente tramite la standardizzazione di:

– protocolli di comunicazione IP: definisce il protocollo comune per lo scambio di informazioni tra dispositivi video di rete tra cui rilevamento dei dispositivi automatici, streaming video e metadati intelligenza.
– rilevamento dei dispositivi;
– assegnazione degli indirizzi IP;
– controllo e configurazione dei dispositivi remoti;
– protocolli dei flussi audio-video;
– visualizzazione e registrazione dei flussi audio-video

La piattaforma DVMS è in grado di realizzare l'integrazione con le reti di videosorveglianza di terze parti anche attraverso la disponibilità di API (Application Programming Interface) sviluppate ad hoc.

Il DVMS RAS dispone di un'interfaccia video in uscita conforme a ONVIF che abilita l'integrazione standardizzata e sicura e assicura l'interoperabilità video completa in installazioni multi-fornitore, fornendo supporto per l'accesso a video live e registrati e la capacità di controllare remotamente le telecamere PTZ (Pan/Tilt/Zoom);

Il DVMS supporta la ricezione, la memorizzazione e l'esportazione dei metadati secondo il formato ONVIF, inclusi i metadati derivanti da sistemi di video analisi residenti a bordo camera e dati di localizzazione dai sistemi mobili.

Adotta lo standard Ethernet TCP/IP e supporta la gestione e la federazione di installazioni con versioni di software anche di release diverse. Fornisce una soluzione avanzata di monitoraggio del sistema, che include la ricezione di notifiche per Allarmi/avvisi per tipologia di oggetto e oggetto singolo, generati da qualsiasi componente del sistema, e avvisi di ritenzione video predittivo.

Il software del sistema DVMS consente l'archiviazione ottimizzate di registrazioni video e audio.

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.

Supporta tutti i protocolli standard. Algoritmi di compressione H.264, H.265, MJPEG, MPEG-4ASP, MxPEG, Zipstream, protocollo di comunicazione unicast, multicast, SNMP, supporto IPV6
A fronte delle caratteristiche del DVMS dell'amministrazione, e tenendo in considerazione le esigenze/richieste di monitoraggio da soddisfare, i sistemi di videosorveglianza locali, realizzati dai soggetti beneficiari dell'intervento "Reti di Sicurezza", devono garantire il rispetto dei requisiti per l'integrazione e l'interoperabilità con esso.
Pertanto per la realizzazione dei sistemi di videosorveglianza locali, da realizzarsi a cura dei beneficiari, si indicano di seguito i requisiti minimi.
1. Garantire la conformità agli standard ONVIF.
2. prevedere l'installazione di telecamere:
a. che consentano l'accesso multiplo, in modo tale che il sistema RAS possa: monitorare e rilevare e gestire gli allarmi, i malfunzionamenti e eventuali manomissioni; intercettare direttamente i flussi video dalle stesse;
b. con adeguato grado di protezione meccanica, per le installazioni esterne e interne, IP66, IP67, IK10 a seconda della tipologia delle telecamere, (meglio declinate nelle tabelle del successivo paragrafo)
c. che, qualora sia previsto il collegamento al sistema centrale attraverso tecnologia radio, siano dotate, on board, di memoria interna in grado di registrare e immagazzinare localmente, in modalità stand alone, le immagini e i flussi video, in caso di malfunzionamento e assenza di segnale radio che impedisca il trasferimento real time dei flussi al sistema centrale di memorizzazione;
d. illuminatori IR, necessari per riprese di aree con scarsa luminosità;
e. funzionalità Day/night;
f. funzione anti accecamento, in particolar modo per telecamere con finalità di rilevamento targhe;
g. preferibilmente con algoritmo di compressione H265, per consentire maggior risparmio di spazio di archiviazione e risparmio del traffico dati consumato.
h. preferibilmente con applicativi di analisi video come, ad esempio: Tripwear, intrusion Abbandoned/missing, face detection;
I sistemi di ripresa soddisfano anche i criteri minimi della circolare N. 558/SICPART/421.2/70 del Ministero dell'Interno in quanto le caratteristiche minime richieste sono per le telecamere di contesto (fisse) e per le telecamere di osservazione (brandeggiabili) sono così riportate:

Telecamere di contesto

Le caratteristiche tecniche degli apparati di ripresa dovranno essere rispondenti alle caratteristiche minime di seguito descritte:
• telecamera IP nativa, aggiornabile via IP;
• ottica fissa intercambiabile o varifocal, da individuare in funzione delle esigenze operative con angolo di ripresa indicativo compreso tra 20° e 120°;
• tecnologia del sistema di ripresa mediante sensore di tipo CMOS o CCD a colori;
• sensibilità del complesso di ripresa almeno 0,5 Lux in modalità colore (day) e almeno 0,05 Lux in modalità B/N (night) misurati a 50 IRE;
• risoluzione minima del sensore: full HD (1920xl080);
• caratteristiche minime del flusso video: 1.3 megapixel (1280xl024) e non inferiore 9 fps;
• modalità di funzionamento di tipo "day&night" con commutazione automatica;
• algoritmo di compressione dei flussi video: Motion JPEG, H264 e sue evoluzioni;
• algoritmo di trasporto dei flussi video: RTSP;
• Funzionalità di Activity Detector incorporate;

• Client NTP;
• n° l ingresso d'allarme a bordo camera;
• n° l uscita;
• controllo del guadagno, white balance: automatici e regolabili via software;
• compensazione del controluce di tipo automatico;
• Possibilità di alloggiare software di analisi video direttamente sulla camera;
• alimentazione: in bassa tensione con valore non superiore ai 48 Vac, PoE classe 3);
• Allarme antimanomissione, al minimo è richiesta la gestione dei seguenti allarmi:
apertura custodia;
perdita del segnale video;
offuscamento telecamera;
modifica dell'inquadratura (spostamento della telecamera)
• condizioni di esercizio: sarà cura della ditta individuare la tipologia di custodia per la singola telecamera in funzione delle condizioni climatiche minime e massime (temperatura, umidità) del luogo di installazione in modo che sia garantito il corretto funzionamento per tutto l'arco dell'anno e comunque in un intervallo non inferiore a (-10°;+45°) e umidità (20%;80%);
• grado di protezione della custodia: l'apparato deve essere protetto dagli agenti atmosferici quali pioggia, salsedine, polveri tipiche del luogo di installazione garantendo così il livello massimo di funzionamento e comunque non inferiore a IP65, eccetto nei casi estremi in cui si richieda una tenuta stagna per cui il valore va esteso a IP66;
• Fornitura SDK per sviluppo terze parti

Telecamere di osservazione

Le telecamere sono brandeggiabili, dovranno assicurare la completa visione a 360° sul piano orizzontale, e 180° sul piano verticale e non dovranno consentire ad un osservatore esterno di individuare l'area inquadrata. Le caratteristiche tecniche degli apparati di ripresa dovranno essere rispondenti alle caratteristiche minime di seguito descritte:
telecamera IP nativa, aggiornabile via IP;
telecamera a colori di tipo "DAY/NIGHT";
matrice attiva del sensore con numero di pixel non inferiore 704 x576 (4CIF);
frame rate non inferiore a 15fps;
sensibilità del complesso di ripresa almeno 0,5 Lux in modalità colore (day) e almeno 0,05 Lux in modalità B/N (night) misurati a 50 IRE;
obiettivo autofocus con zoom (minimo 25X ottico con minimo F.l.8, auto iris);
algoritmo di compressione dei flussi video: Motion JPEG, H264 e sue evoluzioni;
algoritmo di trasporto dei flussi video: RTSP;
brandeggio a velocità variabile orizzontale di tipo endless e verticale controllabile da remoto;
PTZ meccanico;
Funzionalità di Activity Detector incorporate;
Client NTP;
n° 16 Posizioni angolari preselezionabili (Preset);
n° 8 Sequenze di Preset (Tour);
n° l ingressi d'allarme a bordo camera;
almeno n° l uscita d'allarme a bordo camera;
n° 8 Zone di esclusione (Privacy Mask).

Pattugliamento automatico;
alimentazione: in bassa tensione con valore non superiore ai 48 Vac, oppure PoE classe 3);
condizioni di esercizio: sarà cura della ditta individuare la tipologia di custodia per la singola telecamera in funzione delle condizioni climatiche minime e massime (temperatura, umidità) del luogo di installazione in modo che sia garantito il corretto funzionamento per tutto l'arco dell'anno e comunque in un intervallo non inferiore a (-10°;+45°) e umidità (20%;80%);
grado di protezione della custodia: l'apparato deve essere protetto dagli agenti atmosferici quali pioggia, salsedine, polveri tipiche del luogo di installazione garantendo così il livello massimo di funzionamento e comunque non inferiore a IP65, eccetto nei casi estremi in cui si richieda una tenuta stagna per cui il valore va esteso a IP66;
Fornitura SDK per sviluppo terze parti.
Il sistema di registrazione e controllo scelto soddisfa anche i criteri minimi della circolare N. 558/SICPART/421.2/70 del Ministero dell'Interno in quanto definisce le seguenti caratetristiche minime dei videoserver e del sistema di registrazione che vengono così riportate integralmente.

Videoserver

I videoserver devono essere in grado di acquisire, in contemporanea, tutti i flussi provenienti dalle telecamere, che vengono convogliati nel sistema rispettando i seguenti requisiti:
Gestione camere di differenti produttori, piattaforma aperta.
Live View fino a 30 o più FPS;
Gestione dei flussi video con algoritmo di compressione MJPEG/MPEG4/H264;
Funzionalità di NVR;
Esportazione file archiviati con crittografia;
Gestione PTZ Patrolling;
Funzionalità di WEB Client;
Funzionalità di Mobile Client;
Gestione Mappe;
Integrazione con video analisi;
Controllo I/O ed eventi,
Sistemi Operativi di ultima generazione (piattaforme a 64 bit);
Supporto multi stream per camera;
Video Motion Detection (VMD) integrato con gestione zone di esclusione;
Supporto canali audio Full-Duplex;
Preset Positions per camera;
Gestione Preset su Evento;
Preset Patrolling;
Privacy masking;
Ricerca automatica ed auto riconoscimento delle telecamere;
Export e import di configurazioni;
Gestione e esportazione di archivi storici contenenti tutte le informazioni relative agli eventi di stato del sistema e le operazioni compiute dagli addetti (file di log)
Fornitura di SDK per sviluppo applicazioni di terze parti.
I video server hanno un'alimentazione ridondata.

Sistema di Registrazione

Il sistema di registrazione e conservazione dei filmati, anche nell'ottica delle finalità d'impiego da parte dell'Autorità Giudiziaria, deve consentire:

l’archiviazione schedulabile con Playback;
la capacità di registrazione per singola camera con gestione del pre e post allarme;
la memorizzazione delle immagini provenienti da tutte le telecamere al massimo framerate possibile;
l’archiviazione di flussi con algoritmo di compressione MJPEG/MPEG4/H264;
la registrazione delle immagini deve avvenire in forma cifrata per garantirne la riservatezza e l’integrità;
l'esportabilità (da locale o da remoto) dei filmati con corredo di specifico visualizzatore per la decifratura e verifica dell’integrità degli stessi;
la capacità di storage deve essere dimensionata per la registrazione contemporanea di tutte le telecamere al massimo frame rate consentito dalle stesse e/o dalla connettività, per un periodo di almeno 7 gg 24h.

ZONE DI INTERVENTO

1) Ingresso Nord
2) Via Cagliari
3) Piazza di Via Centro
4) Via Centro ingresso ovest
5) SS 442 Ingresso Sud
6) Incrocio SS 442 – Via G. Marconi (Ingresso Est)
7) Via Centro ingresso est
8) Incrocio Via San Giorgio

Tutte le telecamere saranno di tipo speed dome tranne quella posizionata nella corte della casa baronale che sarà una bullet/dome fixed. Come sostegni si utilizzeranno i pali dell’illuminazione pubblica tranne che per il punto 9 (Ingresso Nord) e nel punto 8 (Incrocio via San Giorgio) dove verranno installati due pali ex novo.

Il collegamento all'impianto di videosorveglianza può essere esteso alle Forze di Polizia che ne facciano richiesta all'amministrazione comunale, nei limiti e con l'osservanza delle norme contenute nel presente Regolamento ovvero disciplinate con successivo atto in conformità al quadro normativo di riferimento.

In relazione ai principi di pertinenza e di non eccedenza già richiamati all’art. 2 del presente Regolamento, il sistema informativo ed i programmi informatici 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.

Art. 6 – Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata.

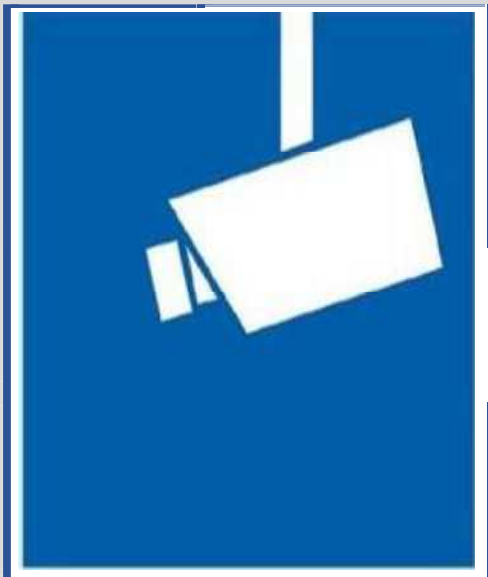
A tal fine il Comune renderà le informazioni di primo livello mediante l’utilizzo di un segnale di avvertimento indicante le informazioni più importanti, quali l’identità del Titolare del trattamento, i dettagli della finalità perseguita, i diritti dell’interessato e le informazioni sui maggiori impatti del trattamento.

Ciò può includere, ad esempio, gli interessi legittimi perseguiti dal Titolare del trattamento (o da una terza parte) e i dettagli di contatto del Titolare della Protezione dei Dati.

L'informativa di primo livello deve comprendere, almeno, l'indicazione dell'eventuale trasmissione di dati a terzi ed il periodo di conservazione dei dati acquisiti mediante l'impianto di videosorveglianza.

Di seguito viene riportato lo schema di informativa di primo livello, come risultante dalle Linee Guida 3/2019 del Comitato Europeo sul trattamento dei dati personali del 10 luglio 2019 approvato il 29 gennaio 2020, e tenuto conto delle disposizioni di cui al già richiamato Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010.

Esempio:



Videosorveglianza!

Dati identificativi del Titolare del trattamento e, ove applicabile, del rappresentante del Titolare del trattamento:

Dati di contatto del Responsabile della Protezione dei Dati (ove applicabile):

I dati acquisiti saranno trasmessi a:

I dati acquisiti saranno conservati su supporti magnetici per "n" giorni e al termine cancellati e non più recuperabili

Finalità e base giuridica del trattamento:

Ulteriori informazioni sono disponibili:

- tramite avviso
- presso la reception / informazioni clienti / registro
- su internet www.xxxxxxxx.xxx

Diritti degli interessati: in quanto soggetto interessato hai diversi diritti nei confronti del Titolare del trattamento, in particolare il diritto di richiedere al Titolare l'accesso o la cancellazione dei tuoi dati personali.

Per i dettagli su questa videosorveglianza, inclusi i tuoi diritti, consulta le informazioni complete fornite dal Titolare attraverso le opzioni indicate a sinistra.

Il Comune, in particolare, provvederà ad affiggere la richiamata segnaletica permanente in corrispondenza di ciascun varco (pedonale e carrabile) di accesso all'area sulla quale insistono gli immobili oggetto di videosorveglianza. Su detta segnaletica è riportata l'informativa come sopra illustrata.

La segnaletica deve essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.
In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi.
Le informazioni di secondo livello devono essere rese disponibili in un luogo facilmente accessibile all'interessato, mediante pannello informativo analogico o digitale. Il segnale di avvertimento di primo livello deve operare un rinvio alle informazioni di secondo livello. Le informazioni del primo livello possono anche fare riferimento a una fonte digitale (ad esempio QR-code o indirizzo di un sito Web) delle informazioni di secondo livello.
In ogni caso, deve essere possibile accedere alle informazioni di secondo livello senza entrare nell'area rilevata. Le informazioni devono contenere tutte le altre informazioni obbligatorie ai sensi dell'articolo 13 del GDPR.

Il Comune, Titolare del trattamento dei dati, si obbliga ad informare gli utenti dei servizi dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un anticipo di giorni dieci, mediante l'affissione di appositi manifesti informativi ovvero mediante comunicazione diretta ai singoli consorziati.

Art. 7 - Valutazione di Impatto sulla protezione dei dati

In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), RGPD, qualora il trattamento di dati realizzato mediante il sistema di videosorveglianza comunale dia luogo ad una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, l'Ente procederà ad una valutazione di impatto sulla protezione dei dati personali.

Parimenti si procederà nei casi in cui, il trattamento di dati realizzato mediante il sistema di videosorveglianza presenti un rischio comunque elevato per i diritti e le libertà delle persone fisiche.

In questa fase di prima attuazione della normativa europea, l'Ente, in conformità al disposto di cui all'art. 35, Paragrafi 4 e 5, RGPD, al fine di avere maggiore chiarezza in relazione ai nuovi adempimenti, attenderà la pubblicazione obbligatoria da parte dell'Autorità Garante per la protezione dei dati personali dell'elenco delle tipologie di trattamenti soggetti alla Valutazione di impatto e l'eventuale pubblicazione dell'elenco delle tipologie di trattamenti per le quali non è richiesta una Valutazione di impatto.

Art. 8 - Titolare del Trattamento

Il Titolare del trattamento dei dati è il Comune di Senis al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.

Art. 9 - Designato a specifici compiti e funzioni connessi al trattamento dei dati

Il Dirigente/Responsabile dell'Area/Servizio/Settore_____(ovvero il Comandante della Polizia Locale) è individuato con decreto sindacale per lo svolgimento di specifici compiti e funzioni di vigilanza e controllo connessi al trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza.

Il Dirigente/Titolare della PO espressamente designato per lo svolgimento di specifici compiti e funzioni di vigilanza e controllo connessi al trattamento dei dati è tenuto a conformare la propria azione al pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente Regolamento.

Il Dirigente/Titolare della PO espressamente designato procede al trattamento dei dati attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

I compiti e le funzioni specifiche attribuite al Dirigente/Titolare della PO espressamente designato al trattamento dei dati personali effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune, sono analiticamente disciplinati nel Decreto con il quale il Titolare provvede alla sua designazione.
In particolare, gli specifici compiti e le funzioni connesse al trattamento dei dati personali attribuiti al Dirigente/Titolare di PO assegnatario dell'esercizio della videosorveglianza sono quelle di seguito indicate:

- fornire al Titolare l'elenco nominativo dei lavoratori che, nell'esercizio dei compiti d'istituto, abbiano accesso ai dati oggetto di rilevazione affinché lo stesso Titolare possa procedere ad adottare l'atto di individuazione di detti lavoratori quali autorizzati al trattamento;
- rendere l'informativa "*minima"* agli interessati secondo quanto definito al precedente art. 6, in conformità alle specifiche tecnico operative del sistema di videosorveglianza;
- provvedere, ad avvenuta individuazione da parte del Titolare degli Autorizzati al trattamento, ad impartire loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, RGPD; dette persone autorizzate saranno opportunamente istruite e formate da parte del Dirigente/Titolare di PO assegnatario dell'esercizio della videosorveglianza con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;
- verificare e controllare che il trattamento dei dati effettuato mediante sistema di videosorveglianza, sia realizzato nel rispetto dei principi di cui all'art. 5 del RGPD e, in particolare, assicurare che i dati personali siano trattati in modo lecito, corretto e trasparente; garantire altresì che i dati personali siano acquisiti e trattati esclusivamente per le finalità connesse all'esercizio dei sistemi di videosorveglianza in quanto determinate, esplicite e legittime;
- assicurare che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

- tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adottare tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;
- assistere il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;
- assistere il Titolare nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 32, RGPD, e coadiuvarlo nella concreta adozione di misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;
- garantire l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, formalizzare tempestivamente la proposta di adozione delle misure necessarie nei confronti dell'Ente;
- assistere il Titolare nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;
- assistere il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e del precedente art. 7 del presente Regolamento e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD;
- affiancare il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del RGPD, nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico;
- fornire al Responsabile per la Protezione dei Dati, ogni elemento, dato e informazione necessari alla regolare formazione, tenuta e all'aggiornamento del Registro delle attività dei trattamenti di cui all'art. 30, paragrafo 1, RGPD.
- garantire che il Responsabile della Protezione dei Dati designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;
- custodire e controllare i dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta
- assicurare che gli autorizzati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantire che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
- garantire la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale individuato quale incaricato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;
- vigilare sul rispetto da parte degli autorizzati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Per l'espletamento dei compiti d'istituto, al Dirigente/Titolare di PO è altresì attribuito il potere di avvalersi di Responsabili del trattamento che, incaricati della **gestione/assistenza del sistema di videosorveglianza** nell'ambito di **incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Ente**, presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato. In questi casi, il Designato al trattamento procederà a disciplinare i trattamenti da parte del responsabile nell'ambito del contratto di affidamento ovvero in altro atto giuridico che vincoli il Responsabile del trattamento al Titolare del trattamento ai sensi dell'art. 28, RGPD.

Art. 9 – Persone Autorizzate al Trattamento

Le persone fisiche autorizzate al trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni, sono individuate con atto del Titolare del trattamento dei dati, ai sensi dell'art. 2 – quaterdecies, comma 2, del D. Lgs. 196/03 e ss.mm.ii. L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato.

In ogni caso, prima dell'utilizzo degli impianti, le persone autorizzate dovranno essere adeguatamente formati sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.

Le persone autorizzate procedono al trattamento attenendosi alle istruzioni impartite dal Dirigente/Titolare di PO il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

In particolare, le persone autorizzate devono:

- per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
- custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- evitare di creare banche dati nuove senza autorizzazione espressa del Dirigente/Titolare di PO al trattamento dei dati;
- mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;
- conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;

- fornire al Dirigente/Titolare di PO ed al Responsabile della Protezione dei dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

Tra i soggetti designati quali autorizzati verranno individuati, con l'atto di nomina, le persone cui è affidata la custodia e la conservazione delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti magnetici.

Le persone autorizzate al trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzione del Titolare o del Dirigente/Titolare di PO.

L'utilizzo degli apparecchi di ripresa da parte delle persone autorizzate al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato.

Art. 10 - Modalità di Raccolta e di Trattamento dei Dati

L'installazione delle telecamere avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili) in conformità all'elenco dei siti di ripresa predisposto dall'Amministrazione Comunale.

L'attività di videosorveglianza deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.

Le telecamere di cui al precedente comma 1, consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.

Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa saranno inviati presso l'Unità di ricezione, registrazione e visione ubicata nell'Ufficio_____. In questa sede le immagini saranno visualizzate su monitor e registrate su supporto magnetico.

I dati personali oggetto di trattamento sono:
- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per le finalità di cui all'art. 4 del presente Regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;
- raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.

La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle richiamate 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 videosorveglianza, fatte salve specifiche esigenze di ulteriore conservazione.

In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria il Titolare del trattamento potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai sette giorni previa richiesta al Garante per la protezione dei dati personali che, a seguito di verifica preliminare, potrà rilasciare parere favorevole.

Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare al momento prefissato l´integrale cancellazione automatica delle informazioni da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati, allo scadere del termine di 7 giorni come previsto dal Provvedimento del Garante della Privacy dell'08 aprile 2010, in ossequio alla finalità di sicurezza urbana di cui all'art. 2 del presente Regolamento.

In caso di cessazione del trattamento, i dati personali sono distrutti.

Art. 11 - Sicurezza dei dati

I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del precedente art. 10.

I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, assicurano:

a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, l'Amministrazione terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ente.

A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini. Tenendo conto dello stato dell'arte ed in base alle caratteristiche dei sistemi utilizzati, i soggetti autorizzati al trattamento, dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le operazioni di competenza;
b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare

non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime immagini operazioni di cancellazione o di duplicazione;

c) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 10, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;
d) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;
e) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;
f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie Wi–Fi, Wi Max, Gprs).

Come già indicato al precedente art. 8, il Titolare del trattamento provvede ad attribuire a persone fisiche espressamente designate, che operano sotto la sua autorità, specifici compiti e funzioni connessi al trattamento di dati personali, nell'ambito dell'Area/Settore di competenza. Parimenti, come indicato all'art. 9, il Titolare provvede ad individuare, sempre in forma scritta, le persone fisiche autorizzate al trattamento ed abilitate ad accedere ai locali dove sono situate le postazioni di controllo, ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

Art. 12 – Accesso ai dati

L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 del presente Regolamento.

L'accesso alle immagini è consentito esclusivamente:

a) al Titolare e alle Persone Autorizzate al trattamento;
b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);
c) alla società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo ovvero, in casi del tutto eccezionali, all'amministratore informatico del sistema comunale (preventivamente individuato quale incaricato del trattamento dei dati);
d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta al successivo art. 13. L'accesso da parte dell'interessato, sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, in conformità alle istruzioni impartite dal Dirigente/Titolare di PO, una

schermatura/sfocatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;

e) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

Art. 13 - Diritti dell'interessato

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD, su presentazione di apposita istanza, ha diritto:

a) di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;

b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;

c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 RGPD, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD.

L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sulla home page del sito istituzionale dell'Ente alla Sezione "Privacy").

Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:

- il luogo, la data e la fascia oraria della possibile ripresa;
- l'abbigliamento indossato al momento della possibile ripresa;
- gli eventuali accessori in uso al momento della possibile ripresa;
- l'eventuale presenza di accompagnatori al momento della possibile ripresa;
- l'eventuale attività svolta al momento della possibile ripresa;
- eventuali ulteriori elementi utili all'identificazione dell'interessato.

Il responsabile della protezione dei dati dell'Ente ovvero il Dirigente/Titolare di PO accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.

Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei *files* contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche

eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD.

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

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.

Art. 14 – Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

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 alle previsioni che saranno contenute nel Decreto Legislativo di prossima emanazione recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE", in attuazione della delega al Governo di cui all'art. 13, L. 163/2017.

Art. 15 – Provvedimenti attuativi

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

Art. 16 – Tutela dell'interessato - Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali

Qualora l'interessato ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, può proporre reclamo al Garante o ricorso dinanzi all'autorità giudiziaria, ai sensi dell'art. 140 – bis del D. Lgs. 196/03 e ss.mm.ii.
Il reclamo al Garante, ai sensi dell'art. 77 del Regolamento UE 2016/679, non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria (art. 140 – bis, comma 2, del D. Lgs. 196/03 e ss.mm.ii).

Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2, RGPD.

Le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli artt. 78 e 79 del Regolamento, nonché il diritto al risarcimento del danno, sono attribuite all'autorità giudiziaria ordinaria (art. 152 del D. Lgs. 196/03 e ss. mm. ii.).

Chiunque ritenga di aver subito un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno ai sensi delle disposizioni di cui all' art. 82, RGPD 2016/679.

Art. 17 - Pubblicità del Regolamento

Copia del presente Regolamento sarà pubblicata all'albo pretorio e potrà essere reperita sul sito internet del Comune.

Art. 18 – Entrata in vigore

Il presente Regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite.
Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.