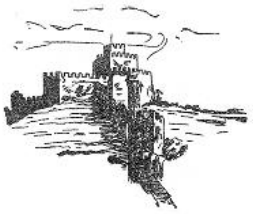
Comune di Soave

Provincia di Verona

POLIZIA LOCALE



REGOLAMENTO SUL TRATTAMENTO DEI DATI PERSONALI MEDIANTE SISTEMI DI VIDEOSORVEGLIANZA

(approvato con deliberazione del Consiglio Comunale n. 16 del 11.09.2020)

INDICE

Art. 1 **Oggetto e norme di riferimento**

Art. 2 **Principi generali**

Art. 3 **Definizioni**

Art. 4 **Finalità istituzionali dei sistemi di videosorveglianza**

Art. 5 **Caratteristiche tecniche dell'impianto**

Art. 6 **Sala controllo**

Art. 7 **Titolare del trattamento**

Art. 8 **Designato al trattamento dei dati**

Art. 9 **Responsabile della protezione dei dati**

Art. 10 **Valutazione d'impatto sulla protezione dei dati e consultazione preventiva con l'Autorità di Controllo**

Art. 11 **Autorizzati al trattamento**

Art. 12 **Accesso ai dati e sicurezza dei dati**

Art. 13 **Obbligo di denuncia da parte di pubblici ufficiali ed incaricati di un pubblico servizio**

Art. 14 **Persone autorizzate ad accedere al locale server dell'impianto di videosorveglianza**

Art. 15 **Accesso ai sistemi a parole chiave**

Art. 16 **Informativa**

Art. 17 **Limiti alla conservazione delle immagini**

Art. 18 **Cautele da adottare per i dati video ripresi**

Art. 19 **Procedura per l’accesso alle immagini**

Art. 20 **Diritti dell’interessato**

Art. 21 **Provvedimenti attuativi**

Art. 22 **Norma di rinvio**

Art. 23 **Pubblicità del regolamento**

Art. 24 **Entrata in vigore**

ALLEGATI AL REGOLAMENTO

Allegato 1 **Fac-Simile della Richiesta di Accesso alle Videoregistrazioni**

Allegato 2 **Foglio tipo per il Registro degli Accessi alla Visione delle Immagini Videoregistrate**

Allegato 3 **Registro attività di trattamento**

Allegato 4 **Registro categorie di attività di trattamento**

Allegato 5 **Modello di cartellonistica informativa**

Art. 1 Oggetto e norme di riferimento

1. Il presente Regolamento disciplina l'esercizio del sistema di videosorveglianza installato nel territorio del Comune di Soave, assicura che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.
2. Garantisce altresì i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento.
3. Stabilisce che l'uso del sistema avvenga nei limiti imposti da:

• Regolamento UE n° 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", recepita nella Legge n° 51 del 2018.
• 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".

Art. 2 Principi generali

1. Il principio di ***liceità***: consente la raccolta e l'uso delle immagini qualora esse siano necessarie per adempiere ad obblighi di legge o siano effettuate per tutelare un pubblico interesse. La videosorveglianza è consentita, senza necessità di alcun consenso, qualora essa sia effettuata nell'intento di perseguire fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, atti di vandalismo, prevenzione di incendi, sicurezza del lavoro.
2 Il principio di ***necessità*** prevede che i sistemi informativi e i programmi informatici vengano configurati riducendo al minimo l'utilizzazione di dati personali/identificativi,

consentendone l’impiego anonimo e solo in caso di stretta necessità. Pertanto, va escluso ogni uso superfluo e vanno evitati eccessi e ridondanze nei sistemi di videosorveglianza; inoltre, qualora non sia necessario individuare le persone (ad es: sistemi di monitoraggio del traffico) i sistemi debbono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, ed il software dei sistemi deve preventivamente essere configurato per cancellare periodicamente e autonomamente i dati registrati.

3. principio di ***proporzionalità***: la raccolta e l'uso delle immagini deve essere commisurato agli scopi perseguiti. Va in generale evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli o per le quali non ricorre un'effettiva esigenza di deterrenza.

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 e controllare.

4. Principio di ***finalità***: gli scopi perseguiti devono essere determinati, espliciti e legittimi ed in ogni caso volti alle finalità indicate all’art. 5 del presente Regolamento (art. 11, comma 1, lettera b) del Codice).

In particolare:

il Comune di Soave intende perseguire, attraverso l’installazione e l’utilizzo di impianti di videosorveglianza, gli obiettivi rispondenti alle funzioni istituzionali proprie demandate all’ente dal D. Lgs 18/08/2000 n°267, dal D.P.R. 24/07/1977 n° 616, dalla L. 07/03/1986 n° 65 e dalle Leggi Regionali in materia di Polizia Locale, nonché dai regolamenti comunali, nei limiti sanciti dal D.lgs. n°196/2003 e dal RGDP, ai quali si rinvia per quanto non è dettagliatamente specificato nel presente regolamento.

Attraverso l’utilizzo del medesimo impianto le forze dell’ordine perseguiranno gli obiettivi rispondenti alle funzioni istituzionali.

Art. 3 Definizioni

Ai fini del presente Regolamento si intende:

a. per "***banca dati***", il complesso di dati personali, formatosi presso la centrale operativa della Polizia Locale, raccolti esclusivamente mediante riprese videoregistrate, che in relazione ai luoghi di installazione delle videocamere interessano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto eventuali;
b. per "***trattamento***", tutte le operazioni svolte con l'ausilio di mezzi elettronici, o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la cancellazione e la distruzione di dati;

c. per "***dato personale***", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente e rilevata con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;
d. per "***titolare***", l'Ente Comune di SOAVE, nella persona del Sindaco o suo delegato, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;
e. per "***designato"***, la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento di dati personali;
f. per "***autorizzati",*** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare e/o dal designato;
g. per "***interessato***" la persona fisica, la persona giuridica, l'ente o associazione a cui si riferiscono i dati personali;
h. per "***comunicazione***", il dare conoscenza dei dati personali a soggetti determinati in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
i. per "***diffusione***", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
j. per "***dato anonimo***", il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non possa essere associato ad un interessato identificato o identificabile;
k. per "***blocco***", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
l. per "***codice***", il D. lgs n° 196/2003 e s.m.i. – Codice in materia di protezione dei dati personali;
m. per "***garante***", l'Autorità di cui all'art. 153 del Codice.
n. per "**responsabile della protezione dati"** figura obbligatoria istituita con RGPD, incaricata di assicurare una gestione corretta dei dati personali negli Enti.
o. per "**registro delle attività di trattamento"** libro in cui descrivere i trattamenti effettuati e le procedure di sicurezza adottate.

Art. 4 Finalità istituzionali dei sistemi di videosorveglianza

1. Le finalità perseguite attraverso l'attivazione di un sistema di Videosorveglianza attengono allo svolgimento delle funzioni proprie dell'Amministrazione comunale previste dalla legge nonché dallo statuto comunale e dai regolamenti comunali vigenti al fine di:

a) Controllare i punti critici della viabilità per definire con precisione gli interventi di polizia stradale, in caso di particolari calamità naturali o di incidenti stradali che prevedano il blocco del traffico.
b) Sorvegliare le zone adiacenti gli uffici comunali, gli edifici di particolare pregio storico ed architettonico ed in genere la tutela del patrimonio pubblico.
c) Monitorare le zone del territorio comunale più soggette a deturpamento mediante abbandono di rifiuti, insudiciamento dell'abitato.

d) Sorvegliare tutte le aree pubbliche ritenute strategiche su tutto il territorio comunale. Solo a titolo esemplificativo e non esaustivo: scuole, aree verdi, parcheggi, cimiteri, campi sportivi, isole ecologiche, etc.

e) agevolare l'Autorità Giudiziaria nello svolgimento di indagini inerenti attività e/o azioni che possono costituire ipotesi di illecito avente rilevanza giuridica;

f) agevolare l'eventuale esercizio in sede giudiziale del diritto di difesa, del titolare del trattamento – o di soggetti terzi - in caso di indagine per ipotesi di reato, tramite l'utilizzo di immagini acquisite.

g) dotarsi di uno strumento attivo di protezione civile sul territorio urbano e di attivazione di misure di prevenzione e sicurezza sul territorio comunale;

h) identificare, in tempo reale, luoghi e ragioni di ingorghi per consentire, fra l'altro, il pronto intervento della Polizia Locale;

i) comunicare agli utenti della strada le vie di maggiore intensità di traffico ed ogni altra notizia utile sulla viabilità;

j) rilevare dati anonimi per l'analisi dei flussi di traffico e la predisposizione dei piani comunali del traffico;

k) prevenire eventuali atti di vandalismo o danneggiamento agli immobili ed in particolare al patrimonio comunale e di disturbo alla quiete pubblica.

2. Il sistema di videosorveglianza deve trattare esclusivamente i dati personali rilevati mediante le riprese televisive e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area interessata.

3. L'installazione delle telecamere avviene nei luoghi pubblici individuati dall'Amministrazione comunale, con apposita deliberazione della Giunta Comunale.

4. L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, limitando l'angolo di visuale delle riprese a quanto strettamente indispensabile. La localizzazione delle telecamere e le modalità di ripresa vanno stabilite in modo conseguente a quanto qui precisato.

5. La possibilità di disporre in tempo reale di dati ed immagini costituisce un ulteriore strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente. Con questi scopi si vogliono tutelare anche le fasce più deboli della popolazione e quindi garantire un elevato grado di sicurezza in particolare negli ambienti circostanti le scuole e comunque in tutti i luoghi di aggregazione.

Art. 5 Caratteristiche tecniche dell'impianto

1. Il sistema si compone di una rete di comunicazione basata su tecnologia via etere, con telecamere fisse e/o brandeggiabili e da sistemi di registrazione digitale che rendono

possibile la visualizzazione di quanto ripreso su personal computer dotati di apposito software gestionale e su sistemi video che potrebbero in futuro essere installati all'interno delle autovetture di servizio.

2. Il sistema può avvalersi di telecamere mobili da posizionare di volta in volta nelle aree sprovviste di punto ripresa fisso per monitorare luoghi in cui si verificano episodi di vandalismo e/o di abbandono di rifiuti.

3. Il sistema non è collegato ad altri apparati né ad alcuna rete pubblica di telecomunicazioni; esso è accessibile solamente dalla centrale operativa ed eventualmente da periferiche autorizzate e dotate di specifica password di accesso ai dati.

4. La relativa password è concessa in uso esclusivo alla Polizia Locale, al Sindaco ed a eventuale delegato alla pubblica sicurezza.

Art. 6 Sala controllo

La sala controllo è ubicata presso la sede della Polizia Locale, alla quale si può accedere tramite una porta di ingresso munita di serratura.

Art. 7 Titolare del trattamento

Il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee, è il Comune di Soave, nella persona del suo Legale Rappresentante pro tempore o suo delegato. Il titolare del trattamento dei dati è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza. A tali fini mette in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali sia 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.

Art. 8 Designato al trattamento dei dati.

1. Designato al trattamento dei dati rilevati con apparecchi di videosorveglianza è il Comandante della Polizia Locale, il quale può delegare in forma scritta le proprie funzioni. Egli vigila sull'utilizzo dei sistemi e sul trattamento delle immagini e dei dati in conformità agli scopi indicati nel presente Regolamento e alle altre disposizioni normative che disciplinano la materia. La nomina avviene mediante apposito atto scritto.

2. I compiti affidati al Designato al trattamento dei dati sono analiticamente specificati per iscritto, in sede di designazione.
3. Il Comandante individua e nomina, con proprio provvedimento, nell'ambito degli appartenenti al Comando di Polizia Locale, gli autorizzati alla gestione dell'impianto nel numero ritenuto sufficiente a garantire la corretta gestione del servizio di videosorveglianza.
Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.
4. Le persone autorizzate del materiale trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni impartite dal titolare o dal designato.
5. Il Comandante designato alla gestione dei dati custodisce le chiavi per l'accesso ai locali della centrale di controllo, le chiavi degli armadi per la conservazione delle immagini, nonché le parole chiave per l'utilizzo dei sistemi.

Art 9 *Responsabile della protezione dati*

In relazione all'attività di videosorveglianza disciplinata dal presente regolamento, il Responsabile della Protezione dei dati / Data Protection Officer è il soggetto individuato dall'Ente ai sensi degli art. 37 e ss. del Regolamento Europeo 2016/679, con i compiti previsti dalla medesima normativa.
Il Responsabile della protezione dei dati è incaricato dei seguenti **compiti**:
a) informare e fornire consulenza al Titolare ed al Responsabile 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 Titolari e/o al Responsabile 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;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità;
f) verificare la tenuta dei registri del Titolare e del/dei Responsabili sul trattamento.

Art.10 Valutazione d'impatto sulla protezione dei dati personali e consultazione preventiva con l'Autorità di Controllo.

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

Art. 11 Autorizzati al trattamento

1. I compiti affidati dal Designato agli autorizzati devono essere specificati nell'atto di designazione.
2. In ogni caso, prima dell'utilizzo degli impianti gli autorizzati vengono istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento e sono obbligati a conformare la loro condotta alle regole ivi contenute.
3. Gli autorizzati procedono al trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.
4. Nell'ambito degli autorizzati vengono 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, alle periferiche ed agli armadi per la conservazione dei supporti magnetici.
5. Gli Incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Titolare o del Responsabile.
6. L'eventuale utilizzo del brandeggio da parte degli autorizzati al trattamento deve essere conforme alle indicazioni riportate nel regolamento.

Art. 12 Accesso ai dati e sicurezza dei dati

I dati registrati possono essere esaminati, nel limite del tempo ammesso per la conservazione, solo in caso di effettiva necessità e per il conseguimento delle finalità di cui all'art. 4 ed esclusivamente dalle Forze di Pubblica Sicurezza, dal Titolare e da ogni altra Autorità Istituzionalmente preposta.
I dati personali oggetto di trattamento devono essere trattati nel rispetto delle indicazioni fornite dal designato alla gestione dei dati e comunque in conformità con i regolamenti e disciplinari interni eventualmente adottati dall'Ente per la protezione delle informazioni e/o l'utilizzo delle strumentazioni date in dotazione.
Il sistema installato adotta le misure di sicurezza volte a ridurre i rischi di distruzione, perdita, anche accidentale delle informazioni, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta dei dati relativi alla videosorveglianza. Tali misure di sicurezza devono essere adottate anche in caso di aggiornamento del sistema.
Il titolare del trattamento prevede una serie di condotte da porre in essere al fine di minimizzare il rischio del trattamento del dato. Tali misure tecniche ed organizzative, attengono alla sicurezza fisica del dato, sono volte a prevenire rischi dipendenti da comportamenti degli operatori e riguardano anche comportamenti da tenere per garantire la sicurezza informatica del dato. Tali misure sono volte anche a consapevolizzare i soggetti deputati al trattamento del dato.
I dispositivi di visualizzazione impiegati per la visione delle immagini, la consultazione ed interrogazione dei dati acquisiti dal sistema sono posizionati e gestiti dagli operatori in modo tale da non permetterne la visione, neanche occasionalmente, a persone estranee non autorizzate.
L'accesso alle immagini da parte dei soggetti indicati nel presente regolamento deve limitarsi alle attività oggetto di videosorveglianza.
Eventuali altre informazioni di cui questi venissero a conoscenza, mentre osservano il comportamento di un soggetto ripreso, devono essere ignorate. Nel caso le immagini siano conservate per una specifica richiesta investigativa dell'autorità giudiziaria o di un organo di polizia giudiziaria, i relativi supporti di memorizzazione (CD/DVD/HD/SD o altri) devono essere custoditi in maniera sicura e accessibili solo al designato al trattamento o alle persone autorizzate.
La cancellazione dei dati avviene con modalità sicure tali da rendere irrecuperabile il dato ed impedirne la disponibilità ad alcun soggetto, anche mediante sovra-registrazione, così come indicato dal Garante per la Protezione dei Dati Personali con Provvedimento del 13 novembre 2007 "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" e con provvedimento dello stesso Garante del 08 aprile 2010 in tema di videosorveglianza

Art. 13 Obbligo di denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio

Qualora dalla visione delle immagini registrate dovessero emergere fatti indicativi di ipotesi di reato, gli Incaricati alla videosorveglianza provvedono immediatamente e senza indugio a darne immediata comunicazione agli organi competenti ai sensi e per gli effetti dell'art. 331 c.p.p. (Obbligo di denuncia da parte di pubblici Ufficiali e incaricati di un pubblico servizio).

Art. 14 Persone autorizzate ad accedere al locale server dell'impianto di videosorveglianza

1. L'accesso al server è consentito esclusivamente al Sindaco pro tempore o ad un suo delegato, al Designato e al personale in servizio della Polizia Locale autorizzato al trattamento dei dati.
2. Il Designato alla gestione e al trattamento impartisce idonee istruzioni, atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso nei locali per le operazioni di manutenzione degli impianti e per la pulizia dei locali, ma non autorizzate al trattamento dei dati stessi.
3. 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.
4. Eventuali accessi a persone diverse da quelle innanzi indicate devono essere autorizzati, per iscritto, dal Sindaco o dal Designato. L'autorizzazione deve contenere anche lo scopo dell'accesso e se possibile il tempo necessario per lo svolgimento dell'attività autorizzata.

Art. 15 Accesso ai sistemi di parole chiave

L'accesso ai sistemi è esclusivamente consentito al Sindaco pro tempore o al suo delegato, al Designato ed agli Autorizzati come individuati nei punti precedenti.
Ciascuno di essi è dotato di un numero identificativo personale e di una chiave di accesso o password personale, di cui è responsabile per la custodia, la conservazione e la assoluta riservatezza.

Le persone autorizzate al trattamento, previa comunicazione scritta al Designato alla gestione e al trattamento dei dati o al Titolare, possono autonomamente variare la propria password al fine di garantirne l'immodificabilità e, in ogni caso, dovranno ottemperare alle istruzioni fornite dal Delegato alla gestione dei dati.
Il sistema è fornito di "log" di accesso, conservati per la durata di 6 mesi.

Art. 16 Informativa

Il Comune di Soave in ottemperanza a quanto disposto dall'art. 13 Regolamento UE 679/2016 è tenuto ad affiggere un'adeguata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere.
Tale supporto con l'informativa deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con le telecamere; deve avere un formato ed un posizionamento chiaramente visibile; può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, in ogni caso in conformità ai provvedimenti vigenti emessi in materia dal Garante per la protezione dei dati personale e alle linee guida del EDPB 3/2008.
Tramite il proprio sito web, l'Amministrazione pubblicizza l'informativa estesa alle procedure di funzionamento del sistema, i servizi attivati, i diritti, i doveri e le modalità di accesso dei cittadini.

Art. 17 Limiti alla conservazione delle immagini

1. Le videocamere rimangono in funzione 24 ore su 24.
2. Eventuali modifiche delle ore di funzionamento sono deliberate dalla Giunta Comunale.
3. La conservazione dei dati, delle informazioni e delle immagini raccolte è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione, nonché in caso si debba aderire a una precisa richiesta della polizia giudiziaria o della magistratura.

Art. 18 Cautele da adottare per i dati videoripresi

1. I monitor degli impianti di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini, neppure occasionalmente, a persone estranee non autorizzate.
2. L'accesso alle immagini da parte del Designato e degli autorizzati al trattamento deve limitarsi alle attività oggetto della sorveglianza: eventuali altre informazioni di cui vengono a conoscenza, mentre osservano il comportamento di un soggetto ripreso, devono essere ignorate.
3. l'accesso alle immagini è consentito solo:
    a) Al Titolare o al suo delegato, al Designato e agli autorizzati allo specifico trattamento;
    b) per indagini alla Autorità Giudiziaria o alla Polizia Giudiziaria;
    c) eventualmente, alla ditta fornitrice/manutentrice dell'impianto, ma solo nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione e previa autorizzazione scritta;
    d) all'interessato debitamente autorizzato in quanto oggetto di ripresa.
4. Nel caso di accesso alle immagini per indagini della Autorità Giudiziaria o di Polizia Giudiziaria, occorre comunque l'autorizzazione da parte del Designato al trattamento o del Titolare;
5. Nel caso di accesso alle immagini da parte del Terzo, debitamente autorizzato, questi può prendere visione solo delle immagini che lo riguardano direttamente;
6. Tutti gli accessi devono essere registrati in un apposito registro, nel quale devono essere riportati:
    - la data e l'ora dell'accesso e di uscita;
    - l'identificazione dell'operatore dell'A.G. o quello della P.G. o del Terzo autorizzato;
    - gli estremi dell'autorizzazione all'accesso;
    - i dati per i quali viene svolto l'accesso;
    - eventuali osservazioni del designato o autorizzato al trattamento dei dati;
    - la sottoscrizione del medesimo.

Non possono essere rilasciate copie delle immagini registrate, salvi i casi in cui è possibile applicare apposito programma oscuratore.
7. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure tecnologiche più avanzate e dovrà essere effettuata esclusivamente sul luogo di lavoro.
8. In caso di sostituzione del supporto di registrazione per usura o guasto, lo stesso deve essere distrutto con conseguente perdita definitiva dei dati ivi contenuti.

Art. 19 Procedura per l’accesso alle immagini

1. Per accedere ai dati ed alle immagini l’interessato deve presentare un’apposita istanza scritta e motivata, indirizzata al Designato, corredata dalla fotocopia del proprio documento di identità.
2. L’istanza deve indicare a quale impianto di videosorveglianza si fa riferimento, il giorno e l’ora in cui l’istante potrebbe essere stato oggetto di ripresa. Nel caso tali indicazioni risultino insufficienti a permettere il reperimento delle immagini, il richiedente viene informato, così pure nell’ipotesi in cui le immagini di possibile interesse non siano state oggetto di conservazione.
3. La risposta all’istanza di accesso ai dati deve essere inoltrata entro quindici giorni dalla ricezione e deve riguardare le immagini attinenti alla persona richiedente. Potrà eventualmente comprendere immagine riferite a terzi solo nei limiti previsti dalla normativa vigente.
4. La Giunta Comunale quantifica, mediante l’adozione di una propria deliberazione, l’eventuale contributo da corrispondere a copertura dei costi sostenuti per l’espletamento della pratica.

Art. 20 Diritti dell’interessato

1. In relazione al trattamento dei dati personali l'interessato identificabile esercita i diritti previsti dal Codice e, come sancito dagli articoli dal 15 al 22 del RGPD 2016/679, il diritto all’accesso, il diritto alla rettifica, il diritto alla cancellazione, il diritto di limitazione di trattamento, con relativo obbligo di notifica da parte del gestore, il diritto alla cancellazione, il diritto alla portabilità dei dati, il diritto all’opposizione. In particolare, ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e la loro comunicazione in forma intelligibile. Può verificare le modalità del trattamento e ottenerne l’interruzione in caso di impiego illecito, soprattutto se le misure di sicurezza dovessero rivelarsi non adeguate.
2. I diritti di cui al presente articolo riferiti a dati personali concernenti persone decedute, possono essere esercitati dagli eredi, da chi abbia un interesse proprio e da chi agisca a tutela dell’interessato.
3. In caso di risposta negativa, l’interessato può rivolgersi al Garante per la protezione dei dati personali.

Art. 21 Provvedimenti attuativi

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

Art. 22 Norma di rinvio

Per quanto non disciplinato dal presente Regolamento si rinvia al Codice in materia di protezione dei dati personali modificato con D.lgs. 51/2018 e D.lgs.101/2018, nonché al provvedimento generale sulla videosorveglianza approvato dall'Autorità garante per la protezione dei dati personali del 08 aprile 2010, eventuali successivi provvedimenti del Garante ed ogni successiva modificazione normativa in materia e al RGPD. 2016/679.

Art. 23 Pubblicità del regolamento

1. Copia del presente Regolamento, a norma dell'art. 22 della legge 7 agosto 1990 n. 241 e successive modificazioni ed integrazioni, è tenuta a disposizione del pubblico perché ne possa prendere visione in qualsiasi momento.
2. Copia dello stesso viene altresì pubblicata all'albo pretorio e sul sito internet del Comune.
3. Copie dello stesso sono trasmesse al Prefetto di Verona, al Procuratore della Repubblica di Verona e al Questore di Verona.

Art. 24 Entrata in vigore

1. Il presente regolamento entra in vigore successivamente alla pubblicazione all'Albo Pretorio nel rispetto dei tempi e delle modalità previsti dalla normativa vigente in tema di pubblicazione degli atti amministrativi.
2. I contenuti del presente regolamento saranno rivisti e adeguati in caso di aggiornamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della protezione dei dati personali o atti regolamentari generali del Consiglio comunale dovranno essere immediatamente recepiti.

3. Il presente regolamento è trasmesso al Garante per la protezione dei dati personali a Roma, sia a seguito della sua approvazione, sia a seguito dell'approvazione di suoi successivi ed eventuali aggiornamenti, laddove ne sussistano i presupposti di legge.

4. Il presente sostituisce integralmente quello approvato con deliberazione del Consiglio Comunale n° 34 del 04.09.2019.

ALLEGATO 1

FAC – SIMILE RICHIESTA DI ACCESSO A VIDEOREGISTRAZIONI

Al Responsabile del Trattamento

Il sottoscritto ……. identificato tramite ……, ai sensi della vigente normativa in materia di privacy richiede di esercitare il diritto di accesso alle immagini video che potrebbero aver registrato dati personali a sé stesso afferenti.
Per permettere di individuare tali immagini nell'archivio video, si forniscono le seguenti informazioni:

1. Luogo o Luoghi di possibile ripresa …….
……..
……..
2. Data di possibile ripresa …….
3. Fascia oraria di possibile ripresa (approssimazione di 30 minuti) ……
4. Abbigliamento al momento della possibile ripresa ……
……..
……..
5. Accessori (borse, ombrelli, carrozzine, animali al guinzaglio, altri oggetti) ……
……..
……..
6. Presenza di accompagnatori (indicare numero, sesso, sommaria descrizione) ……
……..
……..
7. Attività svolta durante la ripresa ……
……..
……..
……..
……..

Recapito (o contatto telefonico) per eventuali ulteriori approfondimenti
……

In fede.

Indicazione del Luogo, della Data, del Nome e del Cognome del Richiedente con firma autografa leggibile
Della richiesta pervenuta il Responsabile del Trattamento deve assicurare formale ricevuta al Richiedente.

ALLEGATO 2

FOGLIO TIPO PER IL REGISTRO DEGLI ACCESSI ALLA VISIONE DELLE IMMAGINI VIDEOREGISTRATE

Nome e Cognome del Soggetto che ha avuto accesso alle immagini: ----------

Documento di identità del suddetto Soggetto: ----------

Estremi della Autorizzazione rilasciata dal Responsabile del Trattamento: ----------

Ora di Entrata: ----------

Ora di Uscita: ----------

Dichiarazione sottoscritta dal Soggetto di cui sopra:

Io sottoscritto ----------, nato a ---------- in data ----------, residente a ----------, domiciliato a ---------- : dichiara, ai sensi della vigente normativa sulla privacy, e sotto la sua personale responsabilità, consapevole delle conseguenze, di mantenere l'assoluta riservatezza su qualunque dato personale di cui possa essere venuto a conoscenza durante la permanenza nel locale.

In fede

Indicazione del Luogo, della Data con firma autografa leggibile