Allegato approvato
con Del. di Consiglio com.le n. 34 del 04/09/2019

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. del)

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	Responsabile del trattamento
Art. 9	Responsabile della protezione dei dati
Art. 10	Valutazione d'impatto sulla protezione dei dati
Art. 11	Incaricati del trattamento
Art. 12	Registro delle attività di trattamento
Art. 13	Registro delle categorie di attività
Art. 14	Accesso ai dati
Art. 15	Obbligo di denuncia da parte di pubblici ufficiali ed incaricati di un pubblico servizio
Art. 16	Persone autorizzate ad accedere al locale server dell'impianto di videosorveglianza
Art. 17	Accesso ai sistemi a parole chiave
Art 18	Informativa
Art. 19	Limiti alla conservazione delle immagini
Art. 20	Cautele da adottare per i dati video ripresi

Art. 21 Procedura per l'accesso alle immagini

Art. 22 Diritti dell'interessato

Art. 23 Sicurezza dei dati

Art. 24 Provvedimenti attuativi

Art. 25 Norma di rinvio

Art. 26 Pubblicità del regolamento

Art. 27 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";
• 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 "***responsabile***", la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento di dati personali;
f. per "***incaricati***", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare dal responsabile;
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 – 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.
p. per "**registro delle categorie di attività**" libro in cui descrivere le categorie di attività trattate dal responsabile, quali: raccolta, registrazione, organizzazione , ecc

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, ecc...

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 delibera 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.

6. L'uso dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali ai sensi dell'art. 18, comma 2, Codice della Privacy.

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 (cioè il Sindaco o suo delegato) dei dati personali raccolti o meno in banche dati, automatizzate o cartacee, 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 per 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 *Responsabile del trattamento*

Uno o più Dirigenti/Quadri/Responsabili di U.O. delle strutture di massima dimensione in cui si articola l'organizzazione del Comune, può essere nominato Responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD. E' consentita la nomina di sub-responsabili del trattamento (gli incaricati del trattamento nel Codice Privacy) da parte di ciascun responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare, dell'inadempimento, dell'operato del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sul suo operato.

Art 9 Responsabile della protezione dati

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.

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
e) trattamenti di dati su larga scala, tenendo conto: del numero dei soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.
Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.
4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.
5.Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
6. La DPIA non è necessaria nei casi seguenti:
- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.
Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con

le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

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

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

10. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 11 INCARICATI DEL TRATTAMENTO

1. I compiti affidati dal Responsabile agli Incaricati devono essere specificati nell'atto di designazione.
2. In ogni caso, prima dell'utilizzo degli impianti gli Incaricati 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 Incaricati 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 Incaricati 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 Incaricati al trattamento deve essere conforme alle indicazioni riportate nel regolamento.

Art. 12 REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Il Registro delle attività di trattamento svolte dal Comune quale Titolare del trattamento, reca almeno le seguenti informazioni:
a) il nome ed i dati di contatto del Comune, eventualmente del Contitolare del trattamento, del RPD;
b) le finalità del trattamento;
c) la sintetica descrizione delle categorie di interessati (cittadini, residenti, utenti, dipendenti, amministratori, parti, altro), nonché le categorie di dati personali (dati identificativi, dati genetici, dati biometrici, dati relativi alla salute);
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati: persona fisica o giuridica; autorità pubblica; altro organismo destinatario;
e) l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Art. 13 REGISTRO DELLE CATEGORIE DI ATTIVITA'

Il Registro delle categorie di attività trattate da ciascun Responsabile del trattamento reca le seguenti informazioni:
a) il nome ed i dati di contatto del Responsabile del trattamento e del RPD;
b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, limitazione, interconnessione, cancellazione o distruzione;
c) l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;
d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve effettuare una valutazione dell'impatto del medesimo trattamento ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

Art. 14 ACCESSO AI 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.

Art. 15 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. 16 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 Responsabile e al personale in servizio della Polizia Locale incaricato del trattamento dei dati.
2. Il Responsabile della gestione e del trattamento impartisce idonee istruzioni, atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso 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 Responsabile. L'autorizzazione deve contenere anche lo scopo dell'accesso e se possibile il tempo necessario per lo svolgimento dell'attività autorizzata.

Art. 17 ACCESSO AI SISTEMI A PAROLE CHIAVE

1. L'accesso ai sistemi è esclusivamente consentito al Sindaco pro tempore o al suo delegato, al Responsabile ed agli Incaricati come individuati nei punti precedenti.
2. Gli incaricati, sono dotati di propria password di accesso al sistema.
3. Il sistema è fornito di "log" di accesso, conservati per la durata di 6 mesi.

Art. 18 INFORMATIVA

Il Comune di Soave in ottemperanza a quanto disposto dall'art. 13 D. Lgs. 196/2003 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.
Il Comune di Soave si obbliga ad attivare una efficace campagna di informazione e comunicazione alla cittadinanza nelle modalità che riterrà più opportune.

Tramite il proprio sito web, l'Amministrazione pubblicizza le procedure di funzionamento del sistema, i servizi attivati, i diritti, i doveri e le modalità di accesso dei cittadini, anche in relazione alla legge sulla privacy.
Trattandosi di svolgimento di funzioni istituzionali, assoggettate dalla legge sulla privacy ad un regime di tipo particolare, l'uso dei dati personali non necessita di preventivo consenso degli interessati, i quali possono avvalersi dei diritti riportati negli articoli dal 15 al 22 del RGPD 2016/679, come indicato nel successivo art. 19 del presente regolamento.

Art. 19 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. 20 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 Responsabile e degli Incaricati del 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 Responsabile e agli Incaricati dello 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;
    d) al Terzo, debitamente autorizzato.
4. Nel caso di accesso alle immagini per indagini della Autorità Giudiziaria o di Polizia Giudiziaria, occorre comunque l'autorizzazione da parte del Responsabile del 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;
- l'identificazione dell'operatore dell'A.G. o quello della P.G. o del Terzo autorizzato;
- gli estremi dell'autorizzazione all'accesso.

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. 21 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 Responsabile, 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. 22 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. 23 SICUREZZA DEI DATI

1. I dati sono protetti da idonee e preventive misure di sicurezza, individuate con documentazione tecnica rilasciata dalla ditta installatrice. Le misure di sicurezza dovranno ridurre al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta.
2. Chiunque tenuto non adempia all'obbligo di adottare le misure minime di sicurezza di cui all'art. 33 del Codice è soggetto alle sanzioni penali previste dall'art. 169 Codice.
3. I dati personali oggetto di trattamento sono custoditi nel server ubicato nella sala di controllo del Comando di Polizia Locale, i sistemi di archiviazione dei dati devono essere custoditi in luogo idoneo.
4. L'utilizzo del videoregistratore non deve consentire la rimozione del disco rigido sul quale sono memorizzate le immagini
5. Il Documento Programmatico di Sicurezza (DPS) deve essere redatto e regolarmente aggiornato dal Comune.

Art. 24 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. 25 NORMA DI RINVIO

Per quanto non disciplinato dal presente Regolamento si rinvia al Codice in materia di protezione dei dati personali approvato con D.L.vo 30 giugno 2003 n. 196, nonché al provvedimento generale sulla videosorveglianza approvato dall'Autorità garante per la protezione dei dati personali del 29 aprile 2004, eventuali successivi provvedimenti del Garante ed ogni successiva modificazione normativa in materia e al R.G.P.D. 2016/679.

Art. 26 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. 27 ENTRATA IN VIGORE

1. Il presente regolamento entra in vigore il trentesimo giorno successivo alla sua pubblicazione all'albo pretorio e sostituisce integralmente quello approvato con deliberazione del Consiglio Comunale n° 37 del 26.11.2015.

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 se 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

REGISTRO ATTIVITA' DI TRATTAMENTO (art. 30, c.1, GPRD)

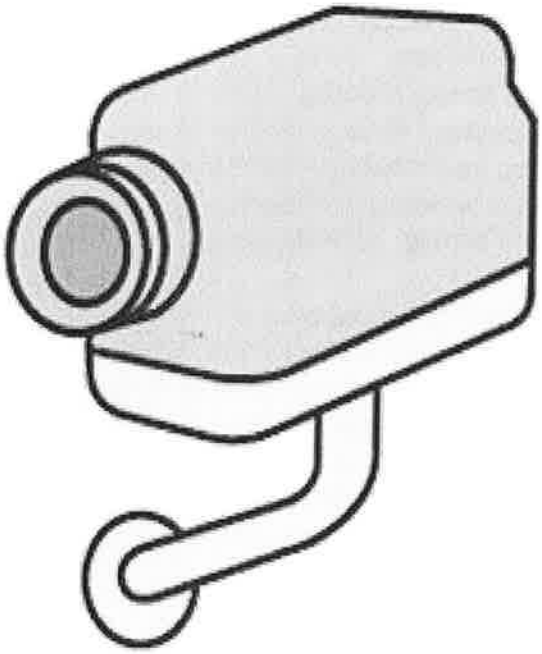
ENTE TITOLARE DEL TRATTAMENTO		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Registro tenuto da**	
Indirizzo		**Data di creazione**	
N. telefono		**Ultimo aggiornamento**	
Mail		**N. schede compilate**	
PEC		**Prossima revisione**	

	TRATTAMENTO			DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Contitolare (eventuale Rappres.nte)	Categoria	Dati sensibili (SI/NO)	Termine ultimo cancell.ne	Categoria	Consenso (SI/NO)	Categoria	Paesi terzi, org.ni int.li (eventuale) (SI/NO)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

REGISTRO CATEGORIE DI ATTIVITA' DI TRATTAMENTO (art. 30, c.2, GPRD)

ENTE TITOLARE DEL TRATTAMENTO		**Responsabile del trattamento**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
		Registro tenuto da	
		Data di creazione	
		Ultimo aggiornamento	
		N. schede compilate	
		Prossima revisione	

	TRATTAMENTO				TRASFERIMENTI	SICUREZZA
n. ordine	**Descrizione**	**Finalità**	**Categorie**	**eventuale diverso Titolare e/o Contitolare (eventuale Rappres.nte)**	**Paesi terzi, org.ni int.li (eventuale)**	**Misure tecniche ed organizzative adottate**



AREA VIDEOSORVEGLIATA

La registrazione è effettuata da ..... per fini di .....

Art. 13 del Codice in materia di protezione dei dati personali D.Lgs. 196/2003
e del Regolamento UE 2016/679 (GDPR)