CITTA' DI SAN MARTINO DI LUPARI
Largo Europa, n. 5 – cap. 35018 Provincia di Padova
Cod. Fiscale 81000530287 -- segreteria@comunesml.info

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI DI VIDEOSORVEGLIANZA URBANA

Approvato con deliberazione

di Consiglio Comunale n. 36 del 29.11.2021

INDICE

CAPO I° - PRINCIPI GENERALI

CAPO II° - SOGGETTI - OBBLIGHI - TRATTAMENTO DATI

CAPO I°

PRINCIPI GENERALI

Art. 1 - Oggetto

1. Il presente regolamento disciplina il trattamento dei dati personali, effettuato mediante gli impianti e sistemi di videosorveglianza (per brevità VS) presenti nel Comune di San Martino di Lupari (per brevità SML), per l'esecuzione di compiti d'interesse pubblico o connessi all'esercizio di pubblici poteri.
2. Per tutto quanto non dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto dalla normativa seguente e successive modifiche e integrazioni (per brevità s.m.i.):
   a) **D. Lgs. n. 101 del 10 agosto 2018** recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"*;
   b) **D. Lgs. n. 51 del 18 maggio 2018** recante: *"Attuazione della direttiva (UE) 2016/680 del Parlamento e del consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, nonché alla libera circolazione dei tali dati e che abroga la decisione quadro 2018/977 GAI del Consiglio";*
   c) **Decreto del Presidente della Repubblica n. 15 del 15 gennaio 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";*
   d) **Regolamento UE n. 679 del 27 aprile 2016** *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;*
   e) **Direttiva UE n. 680 del 27 aprile 2016** *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;*
   f) **Provvedimento Generale sulla videosorveglianza del 08 aprile 2010** *emanato dal Garante per la protezione dei dati personali.*
   g) **D. Lg. N. 11 del 23 febbraio 2009** coordinato con Legge di conversione n. 38 del 23 aprile 2009 recante: "*Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*";
   h) **Provvedimento del 13 novembre 2007** *in materia di "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" emanato dal Garante per la Protezione**;***
   i) **D. Lgs. n. 196 del 30 giugno 2003** "*Codice in materia di protezione dei dati personali*" e s.m.i.;

3. Nell'applicazione del presente regolamento si tiene altresì conto dei principi e delle posizioni espresse dai pareri e dalle linee guida emanate dall'Autorità Garante per la protezione dei dati

personali (GPDP), dell'European Data Protection Board (EDPB) e dall'European Union Agency for Cybersecurity (ENISA).

Art. 2 – Definizioni

Ai fini del presente Regolamento e secondo quanto definito dal Regolamento UE n. 679/2016 si intende:

a. **"archivio"**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
b. **"blocco":** la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
c. **"comunicazione":** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato e persone autorizzate, in qualunque forma anche mediante la loro messa a disposizione o consultazione (art. 2-quaterdecies D.lgs 196/2003 modificato dal D. lgs 101/2018), sotto l'autorità diretta del titolare o del responsabile;
d. **"consenso dell'interessato"**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
e. **"credenziali di autenticazione":** la password ad uso esclusivo di una persona, utilizzata per l'autenticazione di accesso ai sistemi di VS e riconducibile ad uno specifico log identificativo;
f. **"dati biometrici"**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
g. **"dati genetici"**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
h. **"dati personali":** i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché quelli genetici, dati biometrici (intesi a identificare in modo univoco una persona fisica), dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
i. **"dati relativi alla salute"**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
j. **"dati giudiziari":** dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
k. **"dato anonimo":** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
l. **"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;

m. "**destinatario"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
n. **"diffusione":** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
o. **"incaricati del trattamento** (per brevità Incaricati)**":** le persone fisiche autorizzate dal titolare a compiere operazioni di trattamento di dati personali;
p. **"interessato":** la persona fisica cui si riferiscono i dati personali;
q. "**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;
r. "**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;
s. **"responsabile del trattamento"** (data processor - per brevità Responsabile): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
t. **"responsabile della protezione dati** (data protection officier – per brevità DPO.)": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che sovrintende la gestione dell'infrastruttura di videosorveglianza;
u. "**terzo"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare, il Responsabile o gli Incaricati del trattamento dati;
v. **"titolare del trattamento"** (per brevità Titolare): 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;
w. **"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;
x. **"violazione dei dati personali"**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, il blocco o la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Art. 3 - Finalità

1. Il presente Regolamento di VS garantisce che il trattamento dei dati personali si svolga per lo svolgimento delle funzioni istituzionali e nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, persone giuridiche, enti e associazioni, con particolare riferimento alla riservatezza dell'identità personale.

2. Il trattamento dati, oltre a quanto previsto nel precedente art. 1 comma 2°, deve rispettare tutte le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela, oltreché le norme in tema di tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (Statuto dei lavoratori).

3. Gli impianti di VS non potranno essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati per finalità di promozione turistica.

4. In particolare, i sistemi di VS sono utilizzati per:
   a. Protezione e incolumità degli individui (profili di sicurezza urbana);
   b. Supporto al sistema di protezione civile nel territorio e monitoraggio delle aree eventualmente a rischio del Comune;
   c. Ordine e sicurezza pubblica (collegamento e uso degli strumenti in dotazione alle Forze di Polizia);
   d. Prevenzione, accertamento e repressione dei reati o fatti illeciti, con la raccolta degli elementi utili all'accertamento;
   e. Monitoraggio del traffico;
   f. Controllo, prevenzione, accertamento e repressione degli illeciti derivanti dal mancato rispetto delle normative concernenti la tutela ambientale, lo smaltimento e l'abbandono dei rifiuti anche mediante l'utilizzo di telecamere mobili collocate in prossimità dei siti maggiormente a rischio, o utilizzo di telecamere private con uso esclusivo delle registrazioni da parte delle forze di polizia;
   g. Tutela della proprietà:
   h. Tutela del patrimonio pubblico, o dei beni in gestione all'Amministrazione Comunale, prevenzione o accertamento degli atti di vandalismo o danneggiamento;
   i. Contestazione delle sanzioni al CDS nel rispetto della specifica normativa di settore;
   j. Tutela dell'incolumità di soggetti deboli come, ad esempio, minori ed anziani.

5. La normativa in materia di protezione dati, come da nota del GPDP del Dicembre 2020, NON si applica nei seguenti casi:
   a) trattamento di dati che non consentono di identificare le persone, direttamente o indirettamente;
   b) Utilizzo di fotocamere false o spente;
   c) Videocamere integrate in un'automobile per fornire assistenza al parcheggio (se è regolata in modo da non raccogliere informazioni su persone fisiche, targhe o altri dati identificativi).

Art. 4 – Trattamento dei dati personali – Principi applicabili

1. Il trattamento dei dati personali è effettuato mediante l'impianto o sistemi di VS, i cui monitor per la visione delle immagini sono posizionati presso il comando di PL.

2. I dati personali devono essere trattati con i seguenti principi:
   a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
   b. raccolti per finalità determinate, esplicite, legittime e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89 paragrafo 1 del Regolamento UE n. 679/2016, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
   c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
   d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
   e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente al predetto art. 89, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
   f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

3 Il Titolare del trattamento è competente per il rispetto del presente articolo («responsabilizzazione»).

4 L'uso dei dati personali nell'ambito del servizio non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono soggette alla normativa riportata al precedente art. 1.

Art. 5 – Caratteristiche tecniche dell'impianto di VS.

1 Il sistema si compone di una serie di telecamere collegate con rete riservata in fibra ottica alla sede del Comando di PL.; dalla sede del Comando di P.L. è presente un collegamento, sempre in fibra ottica, con la stazione dei Carabinieri di SML., nella quale le persone nominate come "Incaricati" per il trattamento dati, devono rispettare le norme del presente regolamento.

2 Il locale tecnico contenente l'armadio di VS., ubicato all'interno del Palazzo Municipale, è chiuso a chiave e consegnata a specifica persona incaricata, dotata di registro di accesso.

3 Dal punto di vista operativo, l'impianto risulta così organizzato:
   a) Presso il comando di PL. è possibile visualizzare le immagini di tutte le telecamere, brandeggiare e zoomare le telecamere a ciò predisposte.
   b) In caso di necessità è possibile visualizzare le registrazioni dalle telecamere fisse e di quelle mobili. La visione delle immagini potrà avvenire da parte degli incaricati, anche da

remoto a mezzo di applicazione per dispositivi mobili nel rispetto della normativa vigente in materia di privacy;

c) Gli attuali punti di posizionamento delle telecamere di VS sono precisati nel DPIA (Data Protection Impact Assesment) – già approvati in precedenza dall'Amministrazione Comunale e soggetti a modifica da parte della Giunta Comunale.

   Il presente regolamento si colloca nella cornice normativa relativa allo svolgimento delle funzioni istituzionali dell'ente, ai sensi dell'articolo 2 ter, del D. Lgs 30 giugno 2003 n. 196 e s.m.i. / DPIA, che rappresenta il documento di valutazione di impatto sulla protezione dei dati del sistema di VS.

d) Il sistema di VS può essere integrato con l'utilizzo di altri sistemi innovativi di rilevamento targhe, apparecchiature mobili quali bodycam, dashcam, fototrappole, droni e similari laddove tali strumenti siano in dotazione dell'Ente, nel rispetto delle norme tecniche di cui al successivo art. 11 e previa DPIA.

4 Possono essere utilizzate anche strumentazioni messe a disposizione da privati purchè l'uso delle registrazioni sia esclusivo degli Incaricati al trattamento dati e previo specifico accordo scritto tra il Responsabile del sistema di VS ed il proprietario della strumentazione.

Art. 6 - Condizioni di esercizio degli impianti. Valutazione preventiva di impatto.

1. L'attivazione degli impianti di VS è preceduta da una valutazione dell'impatto sulla protezione dei dati e sui diritti e le libertà fondamentali dei soggetti interessati (DPIA), da svolgersi secondo le modalità previste dagli artt. 23 d.lgs. n. 51/2018 e 35 reg. UE 2016/679.

2. La Valutazione di Impatto deve contenere:
   a) una descrizione generale delle caratteristiche degli impianti installati e dei trattamenti previsti l'individuazione dei connessi rischi per i diritti e le libertà degli interessati;

   b) una valutazione in ordine alla conformità del trattamento ai principi fondamentali in materia di protezione dei dati personali, con particolare riferimento alla proporzionalità dei trattamenti ed al loro impatto sugli interessati in relazione alle finalità perseguite;

   c) l'indicazione delle misure organizzative e di sicurezza adottate per assicurare la protezione dei dati personali e la mitigazione dei possibili impatti sui diritti e sulle libertà degli interessati.

3. La Valutazione di Impatto deve essere aggiornata in caso di sostituzione o aggiornamento degli apparati utilizzati o di modifiche ed ampliamenti del sistema di videosorveglianza che diano luogo a cambiamenti sostanziali nelle modalità di trattamento dei dati personali o che determinino trattamenti nuovi, che possano mutare il quadro dei rischi per i diritti o le libertà degli interessati o che rendano necessaria l'adozione di misure tecniche ed organizzative differenti.

4. La valutazione di impatto può prevedere che l'esercizio di sistemi di VS che consentano il trattamento automatizzato delle informazioni raccolte (come, ad esempio, la lettura delle targhe o il riconoscimento facciale) sia subordinata all'approvazione di particolari protocolli tecnici o

l'adozione di particolari misure necessarie a mitigare l'impatto dei trattamenti sui diritti e le libertà degli interessati.

CAPO II°

SOGGETTI - OBBLIGHI - TRATTAMENTO DATI

Art. 7 – Titolare del trattamento dati.

1. Il Titolare del trattamento dati è il Comune di SML, nella persona del Sindaco quale legale rappresentante *pro tempore,* che adempie all'obbligo previsto dall'art. 35 Reg. UE n 679/2016 in tema di valutazione d'impatto sulla protezione dei dati personali, vigilando sulla puntuale osservanza delle disposizioni normative vigenti.

2. Il Titolare 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.

3. Il Titolare nomina il Responsabile del trattamento dati, definendo compiti e priorità, nonchè gli Incaricati del trattamento dati (art. 2 lett. S ed O).

Art. 8 – Responsabile del sistema di VS.

1. Il Comandante della Polizia locale, ovvero altro addetto in caso di sostituzione, è individuato con nomina scritta del Titolare quale Responsabile del sistema di VS, quale delegato di funzioni specifiche ai sensi dell'art. 2-quaterdecies d.lgs. n. 196/2003.

2. In particolare il Responsabile deve:
   a) garantire che gli Incaricati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
   b) verificare che siano adottate tutte le misure richieste ai sensi dell'articolo 32 del suddetto regolamento UE (sicurezza del trattamento);
   c) provvedere a soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al successivo art. 12;
   d) mettere a disposizione del Titolare tutte le informazioni necessarie ad attuare il rispetto degli obblighi di cui al presente articolo e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato.

3. Il Responsabile informa immediatamente il Titolare qualora, a suo parere, una disposizione di quest'ultimo violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati personali.

Art. 9 – Incaricato alla VS.

1. L'Incaricato alla VS, a norma dell'art. 2 quaterdecies del Codice della Privacy è ogni persona che, su apposita nomina di chi esercita la titolarità, potrà compiere trattamenti di dati personali nell'ambito di quanto previsto in questo regolamento.
   Resta inteso che sia il Titolare che il Responsabile possono trattare i dati registrati.

2. Gli Incaricati sono nominati tra gli addetti della PL. di S.M.L. e della stazione dei Carabinieri di S.M.L, che per esperienza, capacità ed affidabilità forniscono idonea garanzia al rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

3. Gli Incaricati sono istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento dal Responsabile, suo delegato o personale incaricato dalla ditta fornitrice del servizio.

Art. 10 – Responsabile della protezione dati

1. In relazione all'attività di VS disciplinata dal presente regolamento, il DPO (Data Protection Officier) è il soggetto individuato dall'Ente ai sensi degli art. 37 e ss. del Regolamento UE n. 679/2016, con le funzioni di garanzia e controllo in materia di riservatezza e tutela dei dati personali previsti dalla medesima normativa.

2. La gestione può essere affidata a consulenti privacy esterni che garantiscono la supervisione dei processi ed il monitoraggio delle problematiche privacy;

Art. 11 - Utilizzo di Bodycam, Dashcam, Fototrappole, Droni e altri dispositivi fissi / mobili – Disposizioni tecniche

1. Le disposizioni di cui al presente regolamento si applicano anche a riprese video e/o acquisizione immagini a mezzo di tablet, bodycam, dashcam, fototrappole, droni e altri dispositivi fissi / mobili il cui fine è inerente all'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di pubblici poteri, come previsto dall'art. 6 paragrafo 1 lett. E del Reg. UE 679/2016. Per l'uso delle dashcam sarà dato avviso con specifiche scritte sulle parti laterali delle auto di servizio.

2. Il Comune di SML all'inizio del territorio Comunale, nelle strade e piazze in cui sono presenti le telecamere, posiziona adeguata segnaletica verticale, chiaramente visibile dall'utenza indicante le principali informazioni previste dall'art. 13 del Reg. UE.

3. Relativamente alle videocamere denominate "bodycam", queste possono essere indossate da ciascun operatore di polizia del comando in via occasionale o continuativa in qualsiasi attività che possa comportare aggressioni o lesioni agli operatori durante il servizio, o per indagini di P.G.. Tali sistemi sono un'estensione delle capacità di acquisizione di atti e fatti a supporto dell'azione di controllo del Comando di P.L.

4. L'uso delle videocamere denominate "dashcam" sulle auto di servizio permette al personale della P.L. di registrare tutta l'attività svolta in pattuglia, quale estensione della capacità di acquisizione di atti e fatti a supporto dell'azione di controllo.

5. L'uso dei dispositivi mobili di videoregistrazione devono rispettare le seguenti modalità tecniche:
   a) Ogni attività di videoregistrazione deve rispettare i principi di cui al precedente art. 4 e, se possibile, informare le persone con le quali si sta operando della registrazione in essere. Non è previsto che gli interessati prestino il loro consenso, rientrando la videoregistrazione tra i compiti di interesse pubblico sopra richiamato.

   b) Dopo ogni utilizzo della bodycam, o altri sistemi di registrazione, la memoria interna della telecamera deve essere formattata per l'uso successivo; i filmati scaricati devono essere criptati e visibili con apposito programma riservato, in modo che la visione sia permessa solo al personale del comando e non anche con normali programmi o supporti commerciali.

   c) Tali filmati possono essere mantenuti su supporto hardware per il tempo necessario al perseguimento delle finalità sottese al trattamento come per le riprese di VS, ai sensi della Legge n. 38/2009 e, al termine, cancellate senza che confluiscano in archivi generici utilizzati per altri scopi.

   d) Per le dashcam che sono installate sulle auto di servizio in via continuativa ed hanno una limitata capacità di memorizzazione, le registrazioni sono sovrascritte automaticamente. In caso di necessità i filmati sono scaricati ed utilizzati con le stesse modalità di cui alle lettere precedenti.

   e) Tutte le persone che effettuano o gestiscono le riprese non possono alterare, duplicare o modificare le immagini o registrazioni.

6. L'uso di droni per registrazioni di VS, oltre al rispetto delle norme di cui al comma precedente, deve essere attuato anche nel rispetto delle disposizioni di cui al Regolamento UE n. 947/2019, Regolamento UAS-IT del 01.04.2021 e s.m.i.

7. L'uso di droni con sistemi di videosorveglianza deve attuarsi con le seguenti modalità:
   a) Evitare di invadere gli spazi personali e l'intimità delle persone, diffondendo le riprese solo con il consenso dei soggetti (se non è possibile ottenerlo, essi non devono essere riconoscibili), evitando di riprendere immagini con dati personali (come targhe di veicoli, indirizzi di casa, etc.), non violando mai gli spazi privati altrui.

   b) Non captare le conversazioni altrui non inerenti le indagini in corso; in tal caso, i frammenti registrati in modo accidentale, non devono rendere riconoscibile il contenuto e le persone coinvolte.

8 Copia delle immagini o registrazioni possono essere rilasciate agli operatoti di Polizia Giudiziaria (per brevità P.G.) previa richiesta scritta, o a personale civile previo nulla osta dell'Autorità Giudiziaria (per brevità A.G.).

Art. 12 – Modalità di raccolta e conservazione dati personali – Sicurezza dati.

1. I dati personali oggetto di trattamento devono rispettare quanto disposto dall'art. 6 del Reg. UE n. 679/2016 (liceità del trattamento), con le finalità di cui all'art. 3 ed i principi di cui all'art. 4 del presente regolamento.

2. I dati personali sono ripresi attraverso i sistemi di VS, sono conservati per un periodo di tempo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali ed in ogni caso per un periodo non superiore a sette giorni, fatte salve specifiche esigenze in relazione ad illeciti che si siano verificati, indagini dell'A.G., P.G. o di pubblica sicurezza.

3. Ai dati oggetto di trattamento possono accedervi, oltre al Titolare, il Responsabile e gli Incaricati, anche gli addetti alla manutenzione e le persone specificatamente autorizzate dal Responsabile.

4. Gli Incaricati sono dotati di propria password di accesso al sistema. Ogni modifica della password deve essere immediatamente comunicata al Responsabile, pena l'applicazione di sanzioni disciplinari. I Log di accesso saranno conservati per almeno un anno.

5. Gli Incaricati si obbligano a non effettuare delle riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali.

6. I dati sono protetti da idonee strutture con specifiche misure di sicurezza certificate, riducendo al minimo i rischi di distruzione, di perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

7. I dati inerenti le sanzioni del CDS possono essere archiviati in appositi server esterni, appartenenti alle ditte fornitrici del servizio, con specifica criptazione e rispetto delle normative di settore.

8. L'area di ripresa delle telecamere deve essere impostata in modo da consentire il controllo e la registrazione di quanto accade nei luoghi pubblici o aperti al pubblico, con esclusione delle proprietà private.

9. I monitor degli impianti di VS sono collocati in modo da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.

10. L'accesso alle immagini da parte del Responsabile e degli Incaricati si limita alle attività oggetto di sorveglianza; eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione.

11. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure tecnologiche più avanzate. Nel caso il supporto debba essere sostituito, sarà distrutto in modo da renderlo inutilizzabile, affinchè non possano essere recuperati i dati in esso presenti.

12. Nel caso di accesso ai dati da parte dell'interessato questi avrà visione solo delle immagini che lo riguardano direttamente.

13. In caso di rilevazioni di immagini concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza, della tutele ambientale o del patrimonio pubblico, il Responsabile o gli Incaricati possono procedere alla conservazione delle immagini e video riprese per il tempo necessario allo svolgimento dell'attività di polizia.

14. Nel caso in cui il privato chieda un riscontro preventivo sulle riprese di VS rispetto alle quali ha la qualifica di interessato, adeguatamente circostanziato, sull'esistenza di elementi utili per procedere con successivi atti, al fine di evitare inutili attività burocratiche, si può "dare riscontro all'istante sul fatto che il dato/le riprese, per cui si chiede il blocco, esistono".

15. In caso di danneggiamento di opere o strutture pubbliche, anche a seguito di incidenti stradali, è possibile chiedere i dati del responsabile al proprietario del veicolo autore del danno , risultante dai registri PRA-MCTC.

16. E' possibile disporre il blocco delle riprese per un certo periodo di tempo (es. prescrizione, termine presentazione querela), eventualmente rinnovabile, a fronte di una specifica richiesta dell'interessato, supportata da adeguata motivazione.

17. E’ in ogni caso fatta salva la comunicazione di dati a Forze di Polizia, all’A.G. o ad altri soggetti pubblici ai sensi dell’articolo 58, comma 2, del D. Lgs. 196 del 30/6/2003 per finalità di difesa di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

18. A norma dell’art. Art 89 del Reg. UE, il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità al regolamento UE. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione purché le finalità in questione siano conseguite attraverso un trattamento che non consenta più di identificare l'interessato.

Art. 13 – Diritti dell'interessato

1. Oltre a quanto previsto dall’art 12 del Regolamento UE n. 679/2016, l'interessato ha il diritto di ottenere dal Titolare 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 personali e alle seguenti informazioni:
   a. le finalità del trattamento;
   b. le categorie di dati personali in questione;
   c. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   d. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   e. l'esistenza del diritto dell'interessato di chiedere al Titolare la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
   f. il diritto di proporre reclamo a un'autorità di controllo;
   g. l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22 del Reg. UE e, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate, ai sensi dell'articolo 46 del Reg. UE relative al trasferimento.

3. Il Responsabile fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il Responsabile può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Relativamente al diritto di limitazione del trattamento dati inerente l’interessato, vedasi quanto disposto dall’art. 18 del Reg. UE n. 679/2016 e s.m.i.

Art. 14 – Cessazione dell'attività di VS

1. In caso di cessazione per qualsiasi causa dell'attività di VS, il Comune di SML effettuerà la notificazione al Garante, se previsto, in base alla normativa al tempo vigente.

2. A seguito di ciò i dati raccolti saranno distrutti o conservati per fini esclusivamente istituzionali salvi i periodi di conservazione previsti dal presente regolamento.

Art. 15 – Tutela amministrativa e giurisdizionale

1) Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia a quanto previsto dagli artt. 140 bis e seguenti del decreto legislativo n. 196 del 30 giugno 2003, così come modificato dal D.lgs. 101/2018.

2) In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge n. 241 del 7 agosto 1990, è il Responsabile del trattamento dati.

Art. 16 – Entrata in vigore.

1. Il presente regolamento entra in vigore il giorno successivo alla pubblicazione all'Albo Pretorio del Comune di SML della delibera di approvazione e sarà pubblicato nella sezione "amministrazione trasparente".

2. I contenuti del presente regolamento sono aggiornati nei casi di significative variazioni normative 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.

a. E' abrogato il precedente "Regolamento per l'utilizzo dell'impianto di videosorveglianza urbana" approvato con deliberazione del Consiglio Comunale n. 11 del 08.04.2014.