



COMUNE DI PALMI
(Città Metropolitana di Reggio Calabria)



REGOLAMENTO PER LA DISCIPLINA DEI SISTEMI DI VIDEOSORVEGLIANZA

Approvato con delibera di Consiglio Comunale n. 34 del 12.06.2024

Indice

Articolo 1 – Premessa

Articolo 2 – Oggetto e definizioni

Articolo 3 – Principi generali e finalità

Articolo 4 – Soggetti

Articolo 5 – Informativa

Articolo 6 – finalità dei sistemi e architettura degli impianti

Articolo 7 - Videosorveglianza partecipata

Articolo 8 – Trattamento e conservazione dei dati

Articolo 9 – Modalità di raccolta dei dati

Articolo 10 – Conservazione dei dati personali

Articolo 11 - Diritti dell'interessato

Articolo 12 – Accesso ai filmati

Articolo 13 - Sicurezza dei dati

Articolo 14 – Cessazione del trattamento dei dati

Articolo 15 – Tutela amministrativa e giurisdizionale

Articolo 16 – Modifiche regolamentari

Art. 1 Premessa

1. Il presente regolamento disciplina le modalità di raccolta, trattamento, conservazione ed accesso dei dati personali mediante sistemi di videosorveglianza gestiti, nell'ambito del territorio comunale ed ha lo scopo di stabilire norme tecniche e organizzative di dettaglio e di concorrere a definire la base giuridica, le finalità e i mezzi del trattamento.
2. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, ossia a distanza, mediante dei dispositivi di ripresa video, collegati ad un centro di controllo.
3. Le immagini, qualora rendano le persone identificate o identificabili, costituiscono dati personali e in tali casi la videosorveglianza incide sul diritto delle persone alla propria riservatezza. Con il presente regolamento si garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti e impiegati dal Comune nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; si garantiscono, altresì, i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento, avuto riguardo anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico.
4. Ai fini delle definizioni si deve fare riferimento al Regolamento UE 679/2016, al Decreto Legislativo. 30 giugno 2003, n. 196, relativi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e al Decreto Legislativo 18 maggio 2018, n. 51 che ha recepito la direttiva Ue 2016/680 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.
5. Il presente regolamento, ai sensi dell'articolo 5 del Regolamento Ue 2016/679 e articolo 3 del Decreto Legislativo. 51/2018, stabilisce norme di dettaglio rilevanti finalizzate ad attuare, a riguardo dei trattamenti dei dati personali effettuati mediante l'uso di sistemi di videosorveglianza, i principi, come definiti nei richiamati articoli 5 e 3, di liceità, correttezza, trasparenza, limitazione delle finalità e minimizzazione dei dati, esattezza, limitazione della conservazione, integrità riservatezza e responsabilizzazione.
6. Il Comune promuove la sottoscrizione di protocolli di intesa, patti per la sicurezza e patti per l'attuazione, convenzioni o accordi comunque denominati con soggetti pubblici e soggetti privati.

Art. 2 Oggetto e definizioni

1. Ai fini del presente regolamento si intende:
 - a) **«impianto di videosorveglianza»:** qualunque impianto di ripresa, fissa o mobile, composto da una o più telecamere, in grado di riprendere e registrare immagini, ed eventualmente suoni, utilizzato per le finalità indicate al successivo art. 3;
 - b) **«banca dati»:** il complesso organizzato di dati personali, acquisiti mediante l'utilizzo di apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle videocamere, riguardano prevalentemente i soggetti ed i mezzi di trasporto che transitano nelle aree interessate dalle riprese;
 - c) **«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. In particolare con trattamenti effettuati attraverso l'impianto di videosorveglianza;
- d) **«trattamento»**: qualsiasi operazione o insieme di attività, 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;
 - e) **«limitazione di trattamento»**: operazione di contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
 - f) **«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 il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
 - g) **«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;
 - h) **«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;
 - i) **«titolare del trattamento»**: Comune di, nelle sue articolazioni interne, cui competono le decisioni in ordine alle finalità e alle modalità del trattamento dei dati personali;
 - j) **«responsabile del trattamento dei dati personali»**: la persona fisica o giuridica, l'autorità pubblica, o altro organismo legato da rapporto di servizio al titolare, che agisce nell'ambito organizzativo per suo conto sotto la sua responsabilità e al quale sono attribuiti specifici compiti e specifiche funzioni connesse al trattamento dei dati personali (es. società che effettuano la manutenzione agli impianti di videosorveglianza);
 - k) **«responsabile della protezione dei dati personali»**: la persona fisica o giuridica, l'autorità pubblica, o altro soggetto legato da contratto di servizio al titolare del trattamento o del responsabile del trattamento, individuato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Regolamento;
 - l) **«responsabile della gestione tecnica degli impianti di videosorveglianza o amministratore di sistema»**: la persona fisica, legata da rapporto di servizio al titolare e preposta dal medesimo all'installazione ed alla manutenzione degli impianti di videosorveglianza;
 - m) **«autorizzati»**: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile del trattamento dei dati personali;
 - n) **«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;
 - o) **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le

- persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del funzionario designato al coordinamento delle attività e al controllo;
- p) **«interessato»**: la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
 - q) **«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;
 - r) **«comunicazione»**: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
 - s) **«diffusione»**: il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
 - t) **«dato anonimo»**: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
 - u) **«violazione dei dati personali»**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
 - v) **«rappresentante»**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento, rappresentante del Titolare;

Art. 3 Principi generali e finalità

1. Ai sensi della vigente normativa in materia di sicurezza urbana i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per tutela della sicurezza urbana, la cui definizione è stata da ultimo riformulata dal Decreto Legge 20 febbraio 2017, n. 14 "Disposizioni urgenti in materia di sicurezza delle città", convertito nella Legge 18 aprile 2017, n. 48, all'articolo 4 e definita come il bene pubblico che afferisce alla vivibilità e al decoro delle città da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio da potenziare con accordi/patti locali ispirati ad una logica di gestione consensuale ed integrata della sicurezza. Si riassumono di seguito i principi per il trattamento dei dati che saranno garantiti scrupolosamente:
 - **Principio di liceità**: il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Esso, infatti, è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui i comuni e il comando di polizia locale sono investiti.
 - **Principio di necessità**: i sistemi di videosorveglianza sono configurati per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
 - **Principio di proporzionalità**: nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra una

effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri accorgimenti.

- **Principio di finalità:** gli scopi perseguiti devono essere determinati, espliciti e legittimi. È consentita la videosorveglianza come misura complementare volta a tutelare la sicurezza urbana anche nell'ambito di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o comunque con lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.
2. Il trattamento dei dati personali attraverso il sistema di videosorveglianza avviene secondo i principi generali di:
- responsabilizzazione (accountability)
 - nel fornire una garanzia di completa accessibilità alle informazioni che riguardano i cittadini in quanto utenti del servizio (principio di trasparenza);
 - nella capacità effettiva di rendere conto delle scelte fatte, dei comportamenti, delle azioni attuate e di rispondere alle questioni poste dai portatori di interessi generali (principio della responsabilità);
 - nella capacità effettiva di fare rispettare le norme sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori (principio della conformità);
 - protezione dei dati fin dalla progettazione (privacy by design) ovvero la necessità di tutelare i dati personali sin dalla fase di sviluppo, progettazione, selezione di un progetto che comporti l'utilizzo di applicazioni, servizi e prodotti per il trattamento di dati personali, creando sistemi che sin dall'inizio dell'attività limitino possibili violazioni dei dati raccolti (articolo 25 comma 1 del GDPR);
 - protezione dei dati per impostazione predefinita (privacy by default) ovvero la necessità di implementare misure giuridiche, tecniche e organizzative efficaci e adeguate a garantire che siano trattati solo i dati personali necessari per ciascuna finalità specifica del trattamento, con l'impostazione a priori della massima protezione dei dati attraverso il loro minimo trattamento sia in fase di raccolta sia in fase di trattamento successivo all'acquisizione, secondo i principi di necessità e pertinenza (articolo 25 comma 2 del GDPR).

Art. 4 Soggetti

1. **Titolare per il trattamento dei dati** è il Comune di Palmi, nella persona del suo legale rappresentante.
2. Il Comandante del Corpo di Polizia Locale è designato, ai sensi dell'articolo 2-quaterdecies del Decreto Legislativo. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e successive modificazioni e integrazioni, quale **Responsabile del trattamento dei dati** personali rilevati attraverso il sistema di videosorveglianza.
3. Il designato individua e nomina, con proprio provvedimento, gli autorizzati alla gestione dell'impianto nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio.
4. Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.
5. I soggetti esterni incaricati dal Comune a installare e/o mantenere l'impianto di video sorveglianza sono qualificati Responsabili esterni al trattamento ai sensi dell'articolo 28 del Regolamento UE 679/2016 "Regolamento Generale Protezione Dati Personali".

6. I rapporti con i responsabili esterni, ai sensi dell'articolo 28 del Regolamento UE 2016/679, sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli stati membri.
7. La gestione tecnica dell'impianto e la manutenzione ordinaria e straordinaria hardware e software possono essere affidati a personale specializzato di ditta esterna. La figura professionale designata dal Comune alla gestione e alla manutenzione dell'impianto di videosorveglianza o di sue componenti è qualificata Amministratore di Sistema (AdS) in conformità con il provvedimento del 27 novembre 2008 emanato dal Garante della Protezione dei dati personali recante le "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"
8. Il Responsabile del trattamento può procedere a designare un **Responsabile della protezione dei dati** (di seguito DPO o RPD) *«quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali»* (art. 37, paragrafo 1, lett a). Il RPD può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi (art. 37, paragrafo 6) e deve essere individuato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i seguenti compiti:
 - a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
 - b) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
 - c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
 - d) cooperare con l'autorità di controllo; e
 - e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Articolo 5 - Informativa

1. I soggetti interessati che stanno per accedere o che si trovano in una zona videosorvegliata devono essere informati mediante cartelli, nei casi specificamente previsti dalla normativa vigente.
2. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, possono essere installati più cartelli.
3. Sul sito istituzionale del Comune, in apposita sezione dedicata, dovrà essere resa disponibile l'informativa concernente le finalità degli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso

dell'interessato secondo quanto previsto dal Regolamento Ue 2016/679 relativamente alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e al Decreto Legislativo 18 maggio 2018, n. 51 relativamente 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 ogni altra informativa attinente la videosorveglianza.

Articolo 6 - Finalità dei sistemi e architettura degli impianti

1. Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza sono conformi alle funzioni istituzionali attribuite ai comuni. L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre polizie locali e delle forze di polizia a competenza generale, dovrà essere specificamente disciplinato con appositi atti, patti e convenzioni.

2. Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato ai fini di:

SICUREZZA URBANA, con lo scopo di:

- assicurare la protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine ed alla sicurezza pubblica, alla prevenzione;
- la ricostruzione in tempo reale, della dinamica di atti vandalici o azioni di teppismo nei luoghi pubblici di principale frequentazione, per permettere un pronto intervento della Polizia Locale e delle Forze dell'Ordine a tutela del patrimonio pubblico;
- prevenire illeciti e fatti criminosi attraverso un'azione di deterrenza che la presenza delle telecamere di videosorveglianza è in grado di esercitare;
- reprimere i reati e aumentare il livello di percezione da parte dei cittadini dell'efficacia delle misure adottate in materia di sicurezza urbana;
- controllare le aree considerate a maggiore rischio per la sicurezza, l'incolumità e l'ordine pubblico;
- proteggere le proprietà pubbliche, in specie quelle comunali;
- tutelare gli immobili di proprietà, o in gestione, dell'Amministrazione Comunale e gli edifici pubblici (come istituti scolastici, impianti sportivi etc..) e a prevenire eventuali atti di vandalismo o danneggiamento;
- acquisire prove utili per la contestazione di fatti illeciti;

SICUREZZA STRADALE, con lo scopo di monitorare il traffico veicolare con impianti di:

- lettura targhe, che prevedono una rete di telecamere per la lettura ed il riconoscimento delle targhe poste sulle principali arterie di entrata e uscite del territorio del Comune;
- telecamere di contesto, con finalità di analisi dei flussi di traffico;
- verifica, controllo e gestione dell'accesso a zone a traffico limitato;
- rilevazione e accertamento delle violazioni al Codice della Strada e segnalazione automatizzata dei veicoli ricercati;
- registrazioni per il monitoraggio del traffico veicolare conservate in forma di dati anonimi che possono essere utilizzate per studi o ricerche sul traffico;

TUTELA AMBIENTALE, con lo scopo di:

- scoraggiare e prevenire l'increscioso e diffuso fenomeno dell'abbandono di rifiuti e la creazione di "micro discariche" sparse nel territorio comunale. Nonostante, infatti, i numerosi controlli ambientali effettuati vengono con molta frequenza abbandonati rifiuti lungo le strade e nelle loro pertinenze nonché nelle aree verdi, con effetti devastanti sia sul piano della tutela ambientale che della normale convivenza civile;

- per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
 - monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti.
3. L'accesso al sistema di videosorveglianza può essere consentito, esclusivamente per le finalità di Istituto, alle altre forze di Polizia. All'atto dell'accesso i soggetti terzi danno garanzia di osservare le disposizioni previste dal presente regolamento compatibilmente con i rispettivi ordinamenti speciali, nonché in relazione alle disposizioni e agli accessi al sistema di videosorveglianza consentiti dal titolare e/o dal Responsabile del trattamento.
 4. Il Comune può dotarsi di body cam, dash cam, droni, telecamere riposizionabili (anche del tipo foto-trappola), altri dispositivi mobili (anche con generazione di allarmi da remoto per il monitoraggio attivo), gestiti sia in forma diretta che attraverso appalto di servizio. In quest'ultimo caso le persone fisiche dipendenti dalle società affidatarie dovranno essere autorizzate a compiere le operazioni di trattamento dal titolare o dal responsabile del trattamento dei dati personali.
 5. Nei casi di cui al precedente comma e comunque quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA). Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi (articoli 32 e 35 del Regolamento Ue 2016/679).
 6. Per le finalità di SICUREZZA STRADALE, se il servizio di gestione dei verbali (dal data entry alla postalizzazione e notificazione degli atti d'accertamento) è esternalizzato, il titolare o il responsabile del trattamento dei dati personali dovrà autorizzare la società/persona fisica dipendente dalla società affidataria a compiere le operazioni di trattamento.
 7. Nel rispetto delle finalità previste nel presente regolamento, dalle immagini di videosorveglianza potranno essere acquisiti elementi utili alla verbalizzazione di violazioni amministrative, nel rispetto delle vigenti normative e regolamenti.
 8. Fermo restando la competenza tecnica del CPOSP (Comitato di Ordine e Sicurezza Provinciale) e dell'UTG (Ufficio Territoriale di Governo) ogni implementazione del sistema di videosorveglianza dovrà essere preventivamente approvata con una delibera di Giunta che evidenzii il rispetto dei principi fondamentali del Regolamento UE 2016/679 e del Decreto Legislativo 51/2018 ovvero la rispondenza del proposto intervento ai principi di legalità, proporzionalità, necessità, finalità e minimizzazione del trattamento.

Art. 7 - Videosorveglianza partecipata

1. Allo scopo di disporre di una rete capillare di strumenti di controllo del territorio comunale attraverso il ricorso alla tecnologia, viene promossa la videosorveglianza partecipata, che consiste nell'adozione di soluzioni tecnologiche che permettono l'integrazione tra i sistemi di videosorveglianza comunale con quelli dei privati (persone fisiche o giuridiche) che si rendano disponibili a condividere infrastrutture e telecamere proprie per finalità di sicurezza pubblica e controllo del territorio.
2. I soggetti privati possono presentare istanza di partecipazione all'impianto di videosorveglianza comunale, nel rispetto dei principi di cui al presente Regolamento, secondo le condizioni definite dalla Legge n. 48 del 18 aprile 2017, che ha convertito il decreto legge n. 14 del 20 febbraio 2017 "Disposizioni urgenti in materia di sicurezza delle città" partecipando al potenziamento del sistema di videosorveglianza comunale,

acquistando e mettendo a disposizione dell'Ente proprie reti di telecamere da utilizzarsi per il controllo di spazi ed aree pubbliche, anche prospicienti edifici privati.

3. La suddetta collaborazione vuole offrire al privato l'opportunità di fruire di un più alto livello di controllo del territorio, con la finalità di rafforzare la sicurezza urbana nell'area in cui risiede e, contestualmente, di implementare il sistema di videosorveglianza del Comune di Palmi, in una logica di leale collaborazione istituzionale. L'Amministrazione Comunale ha quindi inteso promuovere il ricorso a sistemi integrati/partecipati di videosorveglianza tra diversi soggetti, pubblici e privati, facendo in modo che le immagini riprese vengano rese disponibili, con diverse tecnologie e modalità, alla Polizia Locale e alle altre Forze di Polizia, per le finalità stabilite dalla legge e nel rispetto della disciplina in materia di privacy.
4. La videosorveglianza partecipata può coinvolgere privati, amministratori di condominio, centri commerciali naturali, associazioni di categoria, consorzi, imprese, esercizi commerciali, comitati costituiti fra imprese, professionisti o residenti, pubblici esercizi, enti gestori di edilizia residenziale, enti religiosi ed enti pubblici, anche non economici, enti e associazioni del terzo settore.
5. Per aderire al progetto di "videosorveglianza partecipata" gli interessati devono presentare idonei progetti al Comune di Palmi, da sottoporre alla valutazione del titolare e/o del Responsabile del trattamento, che terrà conto dell'interesse che riveste sotto il profilo della sicurezza urbana il sito su cui si propone di installare le telecamere procedendo, in caso di valutazione favorevole, a stipulare uno schema di convenzione tra l'Ente, nella persona del Responsabile del trattamento dei dati, e i soggetti interessati.
6. Al termine del periodo di validità della convenzione, previo accordo tra le parti, l'amministrazione comunale potrà rinnovare la convenzione alle condizioni stabilite, in caso contrario, sarà compito dell'interessato smantellare l'impianto senza alcun onere per il comune di Palmi, che si riserva la facoltà di rinunciare unilateralmente, in qualsiasi momento, alla sopra citata collaborazione offerta dal soggetto proponente.
7. I progetti ritenuti ammissibili faranno capo ad un referente unico e gli impianti utilizzati, conformi alle disposizioni di legge afferenti la videosorveglianza, dovranno possedere una tecnologia compatibile ed integrabile con il sistema di videosorveglianza comunale, e avere una linea di telecomunicazione idonea ad interconnettersi con la rete comunale.
8. Il proponente è tenuto a sostenere per intero i costi necessari per l'acquisto delle telecamere e degli accessori, per l'installazione, per la manutenzione ordinaria e straordinaria, per l'eventuale sostituzione degli impianti (dovuta a danni provocati da terzi, da eventi meteorologici, da atti vandalici o per vetustà dell'apparecchiatura), per la cartellonistica, per la connessione alla rete tecnologica comunale e per l'alimentazione elettrica dei dispositivi di videosorveglianza ceduti, a titolo gratuito, al Comune di Palmi che ne acquista l'esclusiva disponibilità.
9. Resta ben inteso che i privati non possono vantare alcun titolo o diritto di ingerenza sulle immagini, sulle riprese video, sulla gestione e il trattamento dei dati, sulla tecnologia connessa e sulla gestione dei dispositivi di registrazione, che restano di esclusiva competenza del Comune di Palmi. Le modalità di trattamento e i soggetti autorizzati al trattamento saranno espressamente indicati nella convenzione sottoscritta tra le parti.
10. I titolari di impianti di videosorveglianza privata, già attivi nel Comune di Palmi, che intendano estendere la registrazione di immagini delle proprie telecamere su aree pubbliche, o su aree private ad uso pubblico, potranno proporre al Comune di Palmi un progetto nelle forme disciplinate dal presente articolo in qualsiasi momento dall'entrata in vigore del presente regolamento, comunicando:
 - l'ubicazione dell'impianto;
 - i dati identificativi e la reperibilità del titolare dell'impianto;
 - i dati identificativi e la reperibilità del responsabile del trattamento.

Anche in questo caso le modalità di trattamento e i soggetti autorizzati al trattamento dovranno essere espressamente indicati in atto di convenzione sottoscritto tra le parti.

Articolo 8 - Trattamento dei dati

1. I dati personali oggetto di trattamento effettuato con strumenti elettronici nel rispetto delle misure minime indicate dalla normativa relative alla protezione delle persone fisiche sono:
 - a) trattati in modo lecito e secondo correttezza;
 - b) raccolti e registrati per le finalità di cui al precedente articolo 5 e resi utilizzabili per operazioni compatibili con tali scopi;
 - c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
2. Il Comune adotta una specifica procedura per la gestione degli incidenti di sicurezza / data breach che garantisce il rispetto delle disposizioni del Regolamento Ue 2016/679 e la notifica all'Autorità Garante per la Protezione dei dati personali in caso di violazioni di dati personali.

Articolo 9 - Modalità di raccolta dei dati

1. I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da sistemi di telecamere installate in luoghi pubblici ed aperti al pubblico nonché in immobili di proprietà comunale, ubicati nel territorio di competenza.
2. Le telecamere di cui al precedente comma, finalizzate alla tutela della sicurezza urbana, consentono riprese video anche con utilizzo di algoritmi, possono essere dotate di brandeggio e di zoom ottico e sono collegate alla centrale operativa del Comando di Polizia Locale, che potrà, esclusivamente per il perseguimento dei fini istituzionali, eventualmente digitalizzare o indicizzare le immagini.
3. Le immagini videoregistrate sono conservate per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, ed in ogni caso pari al periodo di tempo indicato nel successivo art.10.
4. Le telecamere del "sistema di lettura targhe" sono apparati OCR con illuminatore ad infrarosso che al transito di un veicolo ne fotografano la targa e tramite un software integrato ne leggono il contenuto estraendone la stringa di caratteri alfanumerici. I dati sono interfacciati con le principali banche dati già in uso alla Polizia Locale, per le finalità istituzionali, con particolare riguardo all'attività di accertamento e sanzione delle violazioni di carattere amministrativo previste dal Codice della Strada e/o dalle leggi vigenti. E' fatto salvo l'utilizzo per attività di Polizia Giudiziaria.

Specifiche per il contrasto all'abbandono dei rifiuti

5. In applicazione dei principi richiamati di liceità, finalità e proporzionalità, l'utilizzo dei sistemi di videosorveglianza in riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiale, abbandono di rifiuti e/o sostanze pericolose, o al gettito indiscriminato di rifiuti sulla pubblica via, risulta lecito nell'impossibilità di ricorrere a strumenti e sistemi di controllo e accertamento alternativi o non efficaci.
6. Analogamente, l'utilizzo dei sistemi di videosorveglianza è lecito se non sono attuabili altre misure per monitorare il rispetto delle disposizioni concernenti modalità, tipologia e d orario di deposito dei rifiuti.
7. Per tali finalità nel rispetto dei principi già illustrati nel presente Regolamento, potranno essere utilizzate fotocamere AFC di tipo riposizionabile o modulari (fototrappole) in grado

di effettuare la registrazione anche in notturna. Le telecamere sono corredate di apposito software per il controllo da remoto disponibile per PC.

8. Il trattamento dei dati personali per le finalità sopra esposte, costituisce trattamento dei dati personali e non forma oggetto di disciplina specifica, si applicano, pertanto, le disposizioni generali in tema di protezione dei dati personali e quelle del presente Regolamento, salvo le seguenti specificazioni:

- vengono raccolti solo i dati pertinenti e non eccedenti per il perseguimento delle finalità previste, tra cui la sicurezza urbana e la tutela ambientale;
- le risultanze fotografiche sono utilizzate solo per accertare violazioni alle disposizioni in materia di utilizzo abusivo delle aree impiegate come discariche di materiali, rifiuti e sostanze pericolose ed alle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti;
- le immagini individueranno esclusivamente gli elementi indispensabili per la redazione del verbale di accertamento delle violazioni, secondo quanto previsto dalla vigente normativa. Le stesse non verranno inviate all'indirizzo del contravventore; ferma restando l'accessibilità degli aventi diritto.
- l'accesso alle immagini delle telecamere o/o foto-trappole può essere richiesto dall'interessato con apposita istanza scritta diretta al Titolare, indicando la motivazione e allegando un documento d'identità. Il Designato del trattamento accerterà l'effettiva esistenza delle immagini e, nel caso di esito positivo, fisserà il giorno in cui l'interessato potrà prenderne visione. Persone o elementi non pertinenti alla violazione, al momento dell'accesso verranno in ogni caso oscurati o resi non riconoscibili;
- le riprese vengono conservate per il periodo strettamente necessario alla contestazione e notificazione della violazione ed alla definizione del possibile contenzioso, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'Autorità Giudiziaria o di Polizia Giudiziaria;
- le aree soggette a controllo recano l'Informativa in ordine alla circostanza che viene svolta, attività di registrazione di immagini e conseguente trattamento dei dati personali, a meno che non esistano finalità di sicurezza o necessità di indagine di Polizia Giudiziaria che la escludano;
- i dati rilevati sono chiaramente accessibili anche per fini di Polizia Giudiziaria e di Pubblica Sicurezza;
- L'accesso al sistema, protetto da password, è consentito esclusivamente al Responsabile del trattamento dei dati e ai soggetti da questo autorizzati.

Art. 10 - Conservazione dei dati personali

1. I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza del territorio, finalizzata alla tutela della sicurezza urbana, sono conservati per un periodo di tempo limitato di sette giorni successivi alla data della rilevazione delle informazioni e delle immagini raccolte, fatte salve speciali esigenze di ulteriore conservazione.
2. Decorso tale periodo, i dati registrati sono cancellati in modalità automatica. I sistemi impiegati sono programmati in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni

supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

3. Appare opportuno precisare che non deve essere sottoposta ad una verifica preliminare del Garante l'esigenza di conservare le immagini anche oltre il periodo di una settimana sopra indicato qualora intervenga una specifica richiesta in tal senso dell'Autorità Giudiziaria o di Polizia Giudiziaria in relazione a un'attività investigativa in corso.
4. Fuori dalle ipotesi previste dal comma 3 del presente articolo, la conservazione dei dati personali per un tempo eccedente i sette giorni è subordinata ad una verifica preliminare del Garante per la protezione dei dati personali.

Articolo 11 - Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto, compatibilmente con i fini investigativi a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati:
 - a. di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;
 - b. di essere informato sugli estremi identificativi del titolare e del designato al trattamento, oltre che sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali ed in generale di tutto quanto previsto dall'articolo 13 del Regolamento Ue 2016/679 e articolo 10 e Decreto Legislativo 51/2018;
 - c. di ottenere:
 - la conferma dell'esistenza o meno di dati personali che lo riguardano;
 - la trasmissione in forma intelligibile dei medesimi dati e della loro origine;
 - la cancellazione nei casi previsti dal Regolamento UE 2016/679 qualora sussista uno dei motivi di cui all'articolo 17 del Regolamento Ue 2016/679, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
 - d. di opporsi, nei casi previsti dal Regolamento UE 2016/679, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'articolo 21 del Regolamento Ue 2016/679. Il designato informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti.
 - e. di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle ipotesi specificate all'articolo 18 del Regolamento Ue 2016/679. In tali casi i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico.
2. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
3. Le istanze sono presentate al titolare o al designato al trattamento.

Articolo 12 - Accesso ai filmati.

1. Al di fuori dei diritti dell'interessato, l'accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente.
2. Ogni richiesta deve essere specifica, formulata per iscritto, motivata ed indirizzata al designato del trattamento dei dati competente entro 3 giorni dall'evento.
3. In linea generale l'accesso alla copia delle immagini è consentita solo previa verifica della

sussistenza di un interesse qualificato ai sensi della Legge 7 agosto 1990, n. 241 “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”. Ogni richiesta verrà, comunque, gestita nel pieno rispetto della disciplina dell’accesso agli atti.

4. Per finalità di indagine, l’Autorità giudiziaria e la Polizia giudiziaria possono richiedere ed acquisire copia delle immagini in formato digitale.
5. Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, copia delle riprese in formato digitale può essere richiesta ed acquisita dall’organo di Polizia Stradale che ha proceduto ai rilievi ed in capo al quale è l’istruttoria relativa all’incidente.
6. Nell’ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell’articolo 391-quater del codice di procedura penale, può richiedere ed acquisire copia delle riprese in formato digitale previo pagamento delle relative spese individuate con apposita deliberazione di giunta comunale sulle tariffe di accesso ai documenti amministrativi.
7. Il cittadino vittima o testimone di reato, nell’immediatezza e comunque non oltre 3 giorni dall’evento, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al designato del trattamento che i filmati siano conservati oltre i termini di legge, per essere messi a disposizione dell’organo di polizia procedente. Spetta all’organo di polizia procedente presentare richiesta di acquisizione dei filmati. Tale richiesta deve pervenire entro tre mesi dalla data dell’evento, decorsi i quali i dati non saranno ulteriormente conservati.
8. In ogni caso di accoglimento delle richieste di cui ai commi precedenti, il personale autorizzato dal designato del trattamento dei dati deve annotare le operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, con lo scopo di garantire la genuinità dei dati stessi.
9. Possono essere divulgate immagini provenienti dagli impianti di videosorveglianza, previa anonimizzazione di ogni dato che consenta l’identificazione dei soggetti.
10. Nel caso le immagini di possibile interesse siano oggetto di conservazione, il richiedente dovrà fornire altresì ulteriori indicazioni, finalizzate a facilitare il reperimento delle immagini stesse, tra cui:
 - il giorno e l’ora in cui l’istante potrebbe essere stato oggetto di ripresa;
 - il luogo ed i luoghi di possibile ripresa;
 - la presenza di altre persone;
 - una descrizione dell’attività svolta durante le riprese.
11. Nel caso che tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò dovrà essere data comunicazione al richiedente. Il funzionario designato accerterà l’effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente entro 15 giorni dalla richiesta. Nel caso di accertamento positivo fisserà altresì il giorno, l’ora ed il luogo in cui il suddetto potrà visionare le immagini che lo riguardano.

Articolo 13 - Sicurezza dei dati

1. I dati raccolti mediante sistemi di videosorveglianza e telecontrollo del territorio sono protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini, secondo le “Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni” di cui alla Direttiva del Presidente del Consiglio dei Ministri 1 Agosto

2015 e, comunque, ai sensi dell'art. 32 Regolamento UE 2016/679. I dati personali oggetto di trattamento sono conservati presso la centrale di registrazione individuata, alla quale può accedere il solo personale autorizzato secondo istruzioni che devono essere impartite dal designato al trattamento dei dati.

2. La trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza è applicata con misure tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie wi-fi, wi-max, Gprs).
3. L'accesso agli ambienti in cui è ubicata una postazione di controllo è consentito solamente al personale autorizzato e per scopi connessi alle finalità previste, nonché al personale addetto alla manutenzione degli impianti, alla pulizia dei locali ed a occasionali motivi istituzionali.
4. Il designato impartisce idonee istruzioni atte ad evitare assunzioni o rilevamenti abusivi di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.
5. Il designato individua e nomina gli autorizzati in numero sufficiente a garantire la gestione del servizio di videosorveglianza.
6. La gestione e l'utilizzo dei sistemi di videosorveglianza aventi finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali è riservata agli organi di polizia locale ed alle forze di polizia a competenza generale, aventi qualifica di ufficiali ed agenti di polizia giudiziaria ai sensi dell'articolo 57 del codice di procedura penale.
7. Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi in base alle differenti dislocazioni territoriali degli stessi.
8. In ogni caso, prima dell'utilizzo degli impianti, essi sono istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento.
9. Gli autorizzati al trattamento sono dotati di proprie credenziali di autenticazione al sistema.
10. Il sistema deve essere fornito di log di accesso, che sono conservati per la durata di mesi sei.

Articolo 14 - Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti, ceduti o conservati secondo quanto previsto dal Regolamento Ue 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, e dall'articolo 2 del Decreto Legislativo 51/2018 relativo 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.

Articolo 15 - Tutela amministrativa e giurisdizionale

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli articoli. 77 e seguenti del Regolamento Ue 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, dagli articoli. 37 e seguenti del Decreto Legislativo 51/2018 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.

2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli articoli 4- 6 della Legge 7 agosto 1990, n. 241, è il designato al trattamento dei dati personali, così come individuato dal precedente articolo 3.

Art. 16 - Modifiche regolamentari

1. I contenuti del presente regolamento dovranno essere aggiornati nei casi di aggiornamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari generali del Consiglio comunale dovranno essere immediatamente recepiti.