



COMUNE DI PARGHELIA
PROVINCIA DI VIBO VALENTIA

DELIBERAZIONE DEL CONSIGLIO COMUNALE N. 10 DEL 25/05/2026

OGGETTO: APPROVAZIONE REGOLAMENTO PER LA VIDEOSORVEGLIANZA E PER L'UTILIZZO DEI SISTEMI DI CONTROLLO DEL TERRITORIO.

L'anno duemilaventisei, il giorno 25 del mese di MAGGIO alle ore 18,00, nella residenza comunale, in apposita sala, regolarmente convocati, si è riunito il Consiglio Comunale in sessione ordinaria.

Fatto l'appello nominale risultano i Signori consiglieri:

| N. | Cognome e Nome | Qualifica | Presente | Assente |
|----|----------------------------|-------------|----------|---------|
| 01 | Antonio Landro | Sindaco | x | |
| 02 | Belvedere Tommaso | Consigliere | x | |
| 03 | Collia Francesco | " | x | |
| 04 | Cutuli Rosa Maria | " | x | |
| 05 | Giacco Michele | " | x | |
| 06 | Vallone Andrea | " | x | |
| 07 | Vallone Gabriele | " | x | |
| 08 | Vallone Lorenzo | " | x | |
| 09 | Vasinton Daniele Antonello | " | x | |
| 10 | Ferrazzo Pasquale | " | x | |
| 11 | Minieri Fabio | " | | x |

Preside la seduta di Consiglio Comunale il Sindaco.

Partecipa alla seduta la Dott.ssa Adriana Avventura, Segretario comunale, anche con funzioni di verbalizzante.

Il Sindaco, accertato il numero legale, consiglieri in carica, dichiara aperta la seduta, sull'argomento inserito all'ordine del giorno, premettendo che sulla proposta della presente deliberazione da parte:

del Responsabile del servizio interessato, in ordine alla regolarità tecnica;
è stato espresso parere favorevole ai sensi dell'art. 49 del D.Lgs. n. 267/2000.

del Responsabile del servizio interessato, in ordine alla regolarità contabile;
è stato espresso parere favorevole ai sensi dell'art. 49 del D.Lgs. n. 267/2000.

Il Consigliere Ferrazzo legge un intervento che deposita agli atti. Il sindaco dice che la scelta di adottare il regolamento non è dipeso dal sollecito della minoranza, quanto dalla necessità di consentire l'operatività della polizia locale. Condivide molte delle affermazioni contenute nel documento della minoranza.

Si passa alla trattazione del punto all'o.d.g.

IL CONSIGLIO COMUNALE

PREMESSO CHE

il Comune, nell'ambito delle proprie funzioni istituzionali, promuove azioni finalizzate alla tutela della sicurezza urbana, della sicurezza stradale, del patrimonio pubblico, dell'ambiente e della vivibilità del territorio;

l'evoluzione tecnologica consente oggi l'impiego di sistemi avanzati di videosorveglianza e controllo del territorio utili al perseguimento delle finalità istituzionali dell'Ente;

tali strumenti costituiscono un importante supporto operativo per la prevenzione e l'accertamento di illeciti, la tutela della sicurezza pubblica e la protezione del patrimonio comunale;

CONSIDERATO CHE

il Regolamento UE 679/2016 (GDPR- General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il maggio 2016, è definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

il Garante per la protezione dei dati personali ha emanato apposita Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali;

ai sensi dell'art.13 della Legge n.163/2017, il Governo ha approvato in via preliminare uno schema di decreto legislativo sia al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 che di abrogare le disposizioni recate dal D.Lgs. 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali;

il Garante per la protezione dei dati personali è intervenuto con propri provvedimenti per dettare disposizioni volte a precisare criteri, finalità, modalità e limiti nell'utilizzo dei sistemi di videosorveglianza;

con il provvedimento di cui alla Deliberazione 8 aprile 2010 - il Garante per la protezione dei dati personali ha ridisciplinato la materia, alla luce degli ultimi interventi legislativi sull'adozione di sistemi di videosorveglianza e del generale e consistente aumento del loro utilizzo. Tale provvedimento, oltre a definire i principi generali e le finalità, ha dettato specifiche disposizioni sulle modalità di utilizzo dei sistemi e degli impianti, determinando altresì misure ed accorgimenti da adottare in relazione a particolari settori.

RILEVATO CHE

al fine di dare piena ed effettiva applicazione al nuovo quadro normativo in materia di privacy, le norme introdotte dal Regolamento UE 2016/679 impongono precisi obblighi organizzativi, procedurali e gestionali ricadenti sui titolari del trattamento dei dati personali, ed in particolare occorre:

- adottare un regolamento denominato "Regolamento per la videosorveglianza e per l'utilizzo dei sistemi di controllo del territorio" oggetto della presente deliberazione;
- individuare le modalità di redazione e divulgazione delle informative e le procedure per l'esercizio dei diritti dell'interessato, nonché le modalità di adempimento agli obblighi in materia di "misure di sicurezza".

il Comune utilizza o potrà utilizzare, nell'ambito delle proprie finalità istituzionali:

sistemi di videosorveglianza fissa e mobile;
sistemi di lettura targhe e controllo accessi ZTL;
fototrappole per il contrasto degli illeciti ambientali;
sistemi aeromobili a pilotaggio remoto (droni/UAS);
dispositivi body cam;
dispositivi dash cam;
ulteriori sistemi tecnologici assimilabili;

alcuni sistemi potranno essere attivati successivamente all'approvazione del presente regolamento in relazione alle esigenze organizzative, operative e tecnologiche dell'Ente;

si rende pertanto necessario adottare un regolamento generale che disciplini in modo coordinato tutte le tecnologie di videosorveglianza e controllo del territorio utilizzate o utilizzabili dal Comune;

RITENUTO

opportuno approvare il "Regolamento per la videosorveglianza e per l'utilizzo dei sistemi di controllo del territorio";

necessario dotare l'Ente di uno strumento regolamentare aggiornato e conforme all'evoluzione normativa e tecnologica;

che il regolamento consenta un corretto equilibrio tra esigenze di sicurezza pubblica e tutela dei diritti e delle libertà fondamentali delle persone;

VISTI

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

Il D.Lgs. 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali"), come adeguato dal D.Lgs. 10 agosto 2018, n. 101;

Il D.Lgs. 18 agosto 2000, n. 267 ("Testo Unico delle leggi sull'ordinamento degli enti locali" - TUEL), con particolare riferimento agli artt. 42 e 50;

Il D.L. 20 febbraio 2017, n. 14 (convertito in Legge 18 aprile 2017, n. 48) recante "Disposizioni urgenti in materia di sicurezza delle città";

I provvedimenti generali e le linee guida del Garante per la protezione dei dati personali, con particolare riferimento alle "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video" dell'EDPB e ai provvedimenti in materia di sistemi di videosorveglianza intelligenti e body-cam;

Il D.Lgs. 30 aprile 1992, n. 285 ("Nuovo Codice della Strada") e relativo Regolamento di esecuzione, per quanto concerne il controllo elettronico degli accessi e delle violazioni stradali;

la normativa nazionale ed europea in materia di videosorveglianza, sicurezza urbana e sistemi aeromobili a pilotaggio remoto (UAS);

ACQUISITI

il parere favorevole di regolarità tecnica ai sensi dell'art. 49 del D.Lgs. 267/2000;

Con voti favorevoli 7, astenuti 2 (Ferrazzo, Vasinton)

DELIBERA

1. DI APPROVARE

il "Regolamento per la videosorveglianza e per l'utilizzo dei sistemi di controllo del territorio", allegato alla presente deliberazione quale parte integrante e sostanziale.

2. DI DARE ATTO CHE

il regolamento disciplina:

i sistemi di videosorveglianza fissa e mobile;

i sistemi di lettura targhe e controllo accessi ZTL;

le fototrappole;

i sistemi aeromobili a pilotaggio remoto (droni/UAS);

le body cam;

le dash cam;

ulteriori sistemi tecnologici assimilabili destinati al controllo del territorio e alla sicurezza urbana.

3. DI PRECISARE CHE

l'attivazione dei singoli sistemi tecnologici sarà subordinata:

alla conformità normativa e tecnica;

all'adozione delle misure di sicurezza previste dalla normativa vigente;

all'effettuazione delle valutazioni d'impatto (DPIA) nei casi previsti;

all'adempimento degli obblighi informativi e documentali previsti dalla normativa in materia di protezione dei dati personali.

4. DI STABILIRE CHE

le modalità tecnico-operative di utilizzo dei sistemi saranno disciplinate mediante apposito disciplinare operativo approvato dalla Giunta comunale.

5. DI DEMANDARE

al Comandante della Polizia Locale di adottare tutte le misure tecniche e organizzative adeguate per garantire che i trattamenti dei dati personali vengono effettuati in conformità alla disciplina europea in ottemperanza alle norme recate dal regolamento citato, l'adozione degli atti conseguenti e l'implementazione delle misure tecniche e organizzative necessarie alla corretta gestione dei sistemi.

6. DI DARE ATTO CHE

il presente regolamento costituisce strumento finalizzato:

alla tutela della sicurezza urbana;

alla protezione del patrimonio pubblico;

al miglioramento della sicurezza stradale;

alla tutela ambientale;

alla prevenzione e accertamento degli illeciti;

alla protezione dei dati personali trattati dall'Ente.

Infine il Consiglio Comunale con voti favorevoli 7, astenuti 2 (Ferrazzo, Vasinton);

7. DI DICHIARARE

la presente deliberazione immediatamente eseguibile ai sensi dell'art. 134, comma 4, del D.Lgs. 267/2000, stante la necessità di garantire l'adeguamento dell'Ente alla normativa vigente in materia di videosorveglianza e protezione dei dati personali.

ALLEGATI

* Allegato A – Regolamento comunale per la videosorveglianza e per l'utilizzo dei sistemi di controllo del territorio.



GRUPPO CONSILIARE GUARDARE AL FUTURO

RELAZIONE REGOLAMENTO VIDEOSORVEGLIANZA.

Signor Sindaco, Presidente del Consiglio, colleghi consiglieri.

Oggi discutiamo un tema delicato e importante: il regolamento sulla videosorveglianza e sull'utilizzo dei sistemi di controllo del territorio.

Sia chiaro sin dall'inizio che questa opposizione non è contraria alla sicurezza urbana, né mette in discussione l'utilità degli strumenti di videosorveglianza quando utilizzati in modo corretto, proporzionato e realmente orientato alla tutela del territorio.

Proprio perché parliamo di sicurezza, privacy e diritti dei cittadini, il nostro compito è verificare che questo regolamento sia costruito con equilibrio, trasparenza e adeguato controllo.

Il primo dato politico è semplice.

Finalmente questa amministrazione arriva su un tema che il gruppo Guardare al Futuro aveva già posto formalmente all'attenzione dell'Ente con il protocollo n. 400 del 23/01/2026, che alleghiamo alla presente relazione.

In quella sede avevamo già chiesto chiarezza su:

- chi può accedere alle immagini;
- quali controlli esistano;
- come venga garantita la tracciabilità degli accessi;
- quale separazione vi sia tra gestione tecnica e indirizzo politico, e quali tutele siano previste per i cittadini e per la corretta gestione dei dati.

Oggi prendiamo atto che almeno parte di questi temi siano finalmente entrati nel dibattito istituzionale.

Tuttavia, resta una prima osservazione politica.

Sarebbe stato opportuno e istituzionalmente corretto aprire un confronto preventivo con il Consiglio comunale e con chi, questi temi, li aveva già sollevati per tempo, anziché arrivare direttamente alla fase conclusiva dell'approvazione.

La sicurezza deve essere una materia di responsabilità condivisa.

Secondo punto.

Questo regolamento non riguarda soltanto le tradizionali telecamere di videosorveglianza.

Disciplina anche droni, body cam, dash cam, fototrappole, lettura targhe e altri strumenti particolarmente delicati.

E proprio per questa ampiezza sarebbe stato auspicabile un confronto ancora più approfondito.

Terzo punto.

Dal testo emerge che il Consiglio approva una cornice generale, mentre molte modalità operative vengono demandate a successivi disciplinari tecnici e atti amministrativi.

Ed è su questo che la nostra attenzione resta alta.

Perché una regolamentazione efficace non deve limitarsi ai principi generali, ma deve garantire che accessi, controlli, responsabilità e verifiche siano realmente chiari, tracciabili e ben definiti.

Il punto non è essere contrari alla videosorveglianza.

Il punto è garantire sistemi ben regolamentati, adeguatamente monitorati e gestiti con il necessario equilibrio tra sicurezza, controllo del territorio e tutela dei diritti.

Noi vogliamo un territorio più sicuro, ma anche un Comune più trasparente, più responsabile e più attento alla corretta gestione di strumenti così delicati.

Per questo continueremo a vigilare su:

chi accede alle immagini,

come vengono registrati gli accessi,

quali controlli interni esistano,

e quale concreta separazione vi sia tra funzione tecnica, amministrativa e indirizzo politico.

Infine, una considerazione politica.

Se oggi si arriva a discutere un regolamento che introduce principi di tracciabilità, responsabilità e limiti, è anche perché questi temi erano stati posti con forza dall'opposizione.

Dispiace, però, che ancora una volta si sia arrivati alla fase finale senza un reale confronto condiviso.

Per queste ragioni, il gruppo consiliare **Guardare al Futuro**, pur riconoscendo la necessità di una disciplina regolamentare del settore, esprime riserve sul metodo seguito e ritiene necessario che l'attuazione concreta di questo regolamento venga monitorata con particolare attenzione.

Non saremo mai contrari alla sicurezza, ma saremo sempre favorevoli a una gestione chiara, tracciabile, equilibrata e pienamente condivisa.

Grazie.

I consiglieri del Gruppo Guardare al Futuro

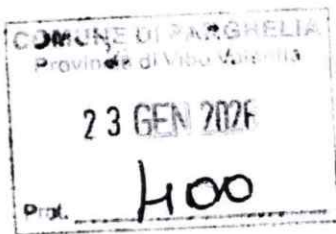
Daniele A. Vasinton



Fabio Minieri

Pasquale Ferrazzo





GRUPPO CONSILIARE GUARDARE AL FUTURO

- Protocollo Comune di Parghelia
protocollo.parghelia@asmepec.it
 - Al Sindaco Antonio Landro
- Al Segretario Comunale Dott.ssa Adriana Avventura
- Al Responsabile dell'Ufficio Legale / Affari Generali
 - Responsabile della Polizia Locale
 - Responsabile della Protezione dei Dati (DPO), se nominato
- Responsabile dell'Ufficio Tecnico

OGGETTO: Richiesta di accesso agli atti – Sistema di videosorveglianza comunale: assetto organizzativo, modalità di utilizzo, soggetti autorizzati e misure di controllo ai sensi della normativa privacy e del Regolamento (UE) 2016/679 (GDPR)

I sottoscritti Consiglieri comunali del gruppo consiliare *Guardare al Futuro*,

PREMESSO CHE

- nel territorio comunale, ed in particolare nel centro abitato, risulta installato e funzionante un sistema di videosorveglianza, composto da più apparati di ripresa e da sistemi di registrazione e gestione delle immagini;
- allo stato attuale, i sottoscritti Consiglieri comunali **non dispongono di informazioni complete, organiche e documentate** circa:
 - le modalità di utilizzo del sistema;
 - i soggetti legittimati ad accedere alle immagini;
 - le finalità concretamente perseguite;
 - l'esistenza di procedure formalizzate, limiti operativi, controlli e sistemi di tracciamento degli accessi;
- allo stato delle informazioni disponibili ai sottoscritti Consiglieri comunali **non risulta adottato alcun regolamento comunale organico** che disciplini in modo puntuale l'utilizzo del sistema di videosorveglianza, le finalità del trattamento, i soggetti autorizzati all'accesso, i limiti operativi, i sistemi di controllo e la separazione tra funzioni tecniche e di indirizzo politico;
- risulta altresì attiva sul territorio comunale una telecamera di videostreaming installata presso la spiaggia di Michelino, destinata alla diffusione in tempo reale delle immagini dell'area costiera;
- anche tale sistema, pur se qualificato come videostreaming e non come videosorveglianza in senso stretto, comporta un trattamento di dati personali e richiede l'esistenza di regole chiare in ordine alla gestione, all'accesso, alle responsabilità e alle misure di sicurezza;
- il diritto di accesso dei Consiglieri comunali agli atti dell'Ente è **rafforzato, immediato e non subordinato ad oneri motivazionali**, ai sensi dell'art. 43 del D.Lgs. 267/2000 (TUEL), ed è funzionale all'esercizio del mandato elettivo e delle funzioni di indirizzo e controllo;

CONSIDERATO CHE

- l'utilizzo di sistemi di videosorveglianza in ambito pubblico costituisce un trattamento di dati personali potenzialmente invasivo, che, ai sensi del Regolamento (UE) 2016/679 (GDPR) e della normativa nazionale vigente, deve essere:
 - fondato su finalità determinate, legittime e documentate;
 - limitato ai principi di necessità, proporzionalità e minimizzazione;
 - accompagnato da adeguate misure di sicurezza, responsabilizzazione e controllo;
- la mancata definizione formale di ruoli, limiti e modalità di accesso alle immagini può determinare rilevanti criticità sotto il profilo:
 - della tutela dei diritti e delle libertà fondamentali dei cittadini;
 - della responsabilità amministrativa e organizzativa dell'Ente;
 - della trasparenza e del corretto esercizio delle funzioni di indirizzo e controllo del Consiglio comunale;

TUTTO CIÒ PREMESSO, I SOTTOSCRITTI CHIEDONO

di poter esercitare il diritto di accesso agli atti e ottenere **copia integrale** della seguente documentazione:

A. Atti istitutivi e organizzativi del sistema

1. atti deliberativi e/o determinazioni dirigenziali relativi all'installazione, all'ampliamento o alla modifica del sistema di videosorveglianza comunale;
2. eventuali progetti, relazioni illustrative, verbali di collaudo e messa in esercizio;
3. contratti, affidamenti o convenzioni relativi alla gestione, manutenzione o assistenza del sistema, inclusi eventuali soggetti esterni coinvolti;

B. Assetto privacy e responsabilità

1. atti di individuazione del Titolare del trattamento e degli eventuali Responsabili del trattamento;
2. registro dei trattamenti (o estratto) relativo alla videosorveglianza;
3. eventuale valutazione d'impatto sulla protezione dei dati (DPIA);
4. informative privacy e cartellonistica adottate;

C. Utilizzo operativo, accessi e controlli

1. regolamento comunale, disciplinare interno o altre disposizioni che disciplinano l'utilizzo del sistema di videosorveglianza (ove esistenti);
2. atti di designazione o autorizzazione dei soggetti abilitati all'accesso al sistema, con indicazione del ruolo, delle funzioni e del profilo di autorizzazione;
3. indicazione di eventuali soggetti titolari di cariche politiche o di governo dell'Ente che risultino autorizzati, direttamente o indirettamente, all'accesso al sistema o alle immagini;
4. eventuale individuazione degli amministratori di sistema;
5. procedure di gestione delle credenziali di accesso (rilascio, revoca, disattivazione);
6. documentazione relativa ai sistemi di tracciamento e registrazione degli accessi (log), con indicazione delle informazioni registrate e dei tempi di conservazione;

D. Rapporti con altri enti

1. eventuali convenzioni, protocolli o accordi con Prefettura, Forze dell'Ordine o altri Enti per la visione o l'utilizzo delle immagini;
2. procedure adottate per l'estrazione, la conservazione e la trasmissione delle immagini a soggetti esterni.

E. Sistema di videostreaming – Spiaggia di Michelino

1. atti autorizzativi e/o deliberativi relativi all'installazione e all'attivazione della telecamera di videostreaming presso la spiaggia di Michelino;
2. individuazione del soggetto responsabile della gestione del sistema (ufficio comunale, soggetto esterno, ditta fornitrice, altro);

3. indicazione del luogo fisico da cui viene gestito il sistema e dei dispositivi utilizzati per l'accesso (PC, tablet, smartphone, server dedicato, cloud, ecc.);
4. modalità tecniche di funzionamento (streaming continuo, possibilità di registrazione, conservazione delle immagini, accesso remoto);
5. indicazione dei soggetti che possono accedere al sistema e delle relative autorizzazioni;
6. eventuali procedure di sicurezza adottate per impedire accessi non autorizzati;
7. informative e cartellonistica riferite specificamente alla presenza della telecamera di videostreaming.

FINALITÀ DELL'ACCESSO

La presente richiesta è finalizzata a consentire ai Consiglieri comunali una **valutazione completa e informata** dell'attuale assetto del sistema di videosorveglianza comunale, al fine di verificare la conformità del sistema ai principi di liceità, necessità, proporzionalità e minimizzazione del trattamento dei dati personali previsti dal Regolamento (UE) 2016/679 (GDPR), nonché l'esistenza di adeguati limiti, controlli e tracciamenti degli accessi e la corretta separazione tra funzioni tecniche, amministrative e di indirizzo politico.

Ciò anche in vista della **predisposizione e proposizione, da parte dei Consiglieri richiedenti, di un regolamento comunale in materia di videosorveglianza**, conforme alla normativa privacy e ai principi del GDPR, nell'esclusivo interesse della tutela dei diritti dei cittadini, della trasparenza amministrativa e del corretto funzionamento dell'Ente.

MODALITÀ DI TRASMISSIONE

Invio in formato digitale (PDF), tramite PEC o altro mezzo concordato, con attestazione di conformità ove necessario.

REGISTRAZIONE E PROTOCOLLAZIONE

Si richiede che la presente istanza:

- sia regolarmente protocollata;
- venga trasmessa agli uffici competenti;
- venga restituita copia recante il numero di protocollo.

I consiglieri del Gruppo Guardare al Futuro

Daniele Antonello Vasinton



Pasquale Ferrazzo



Fabio Minieri





COMUNE DI PARGHELIA

Regolamento per la disciplina ed utilizzo degli impianti di videosorveglianza e per l'utilizzo del controllo del territorio

(Approvato con Deliberazione del Consiglio Comunale 10 del 25/05/2026)

INDICE

CAPO 1- DISPOSIZIONI GENERALI

Art. 1-Oggetto

Art.2-Definizioni

Art.3-Norme di riferimento

Art.4-Principi generali per il trattamento dei dati mediante sistema di videosorveglianza

Art.5-Finalità dei sistemi

CAPO 2- SOGGETTI COINVOLTI NEL TRATTAMENTO

Art.6- Soggetti

CAPO 3- TRATTAMENTO DEI DATI PERSONALI

Art.7- Modalità di raccolta a e requisiti dei dati personali

Art.8-Trattamento e conservazione dei dati

Art.9-Informativa

Art.10-Comunicazione e diffusione dei dati personali a Enti o Organismi pubblici

Art.11-Utilizzo di particolari sistemi

Art.12-Strumenti diversi di rilevazione immagini: body cam e dash cam

Art.13-Utilizzo di sistemi aeromobili a pilotaggio remoto (UAS/DRONI)

Art.14-Cessazione del trattamento dei dati personali

Art.15-Diritti dell'interessato

Art.16-Accesso ai filmati

Art.17-Valutazione di impatto sulla protezione dei dati

Art.18-Utilizzo in ambiente di lavoro

CAPO 4- MISURE DI SICUREZZA

Art.19-Principi generali di sicurezza del trattamento

Art.20-Misure tecniche e organizzative minime

Art.22-Architettura dei sistemi e conservazione dei dati

Art.23-Data breach e gestione delle violazioni di sicurezza

Art.24-Responsabilità del titolare del trattamento

Art.25-Integrazione con i sistemi speciali di videosorveglianza

Art.26-Sicurezza dei dati personali

Art.27-Accesso alle centrali di controllo

Art.28-Accesso logico ai sistemi e ai dati.

Art.29-Sicurezza nelle trasmissioni

Art.30-Utilizzo degli strumenti e dei supporti di memorizzazione

Art.31-Accesso ai dati da parte delle Forze di polizia e Autorità Giudiziaria

CAPO 5- TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art.32-Tutela

CAPO 6- ALTRE DISPOSIZIONI

Art.33-Diritto al risarcimento, responsabilità e danno cagionati per effetto del trattamento dei dati personali

Art.34-Provvedimenti attuativi

Art.35-Modifiche regolamentari

Art.36-Entrata in vigore

Art.37-Norma di rinvio

CAPO 1- DISPOSIZIONI GENERALI

Art.1-Oggetto

1. Il presente regolamento disciplina in modo organico e unitario i sistemi di videosorveglianza e di controllo del territorio attualmente installati o in esercizio sul territorio comunale di Parghelia, nonché quelli che potranno essere attivati in futuro purché riconducibili alle finalità istituzionali indicate dal presente atto e le modalità di raccolta, trattamento e conservazione dei dati personali;

2. Rientrano nel campo di applicazione del presente regolamento, sin dal momento della loro attivazione, tutti i sistemi riconducibili alle seguenti categorie funzionali:

- videosorveglianza fissa e mobile;
- sistemi di controllo elettronico del traffico e della circolazione, incluse le Zone a Traffico Limitato (ZTL);
- sistemi di rilevazione automatizzata (fototrappole e analoghi dispositivi);
- sistemi aeromobili a pilotaggio remoto (droni/UAS);
- dispositivi di ripresa indossabili (body cam);
- sistemi installati su veicoli di servizio (dash cam);
- ogni ulteriore tecnologia assimilabile per finalità e modalità di trattamento dei dati.

3. L'attivazione di nuovi sistemi o tecnologie rientranti nelle categorie di cui al presente articolo non comporta modifica del regolamento, purché:

- siano rispettate le finalità istituzionali già previste;
- siano garantiti i principi di liceità, necessità, proporzionalità e minimizzazione;
- siano adottati gli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali.

Resta fermo che ogni sistema, prima della sua effettiva messa in esercizio, è subordinato alle verifiche tecniche, organizzative e giuridiche previste dalla normativa applicabile, incluse le valutazioni di impatto (DPIA) ove richieste.

4. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, che si realizza a distanza mediante dispositivi di ripresa video, captazione di immagini ed eventuale conseguente analisi, collegati a un centro di controllo;

5. Qualora tali immagini rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi la videosorveglianza incide sul diritto delle persone alla propria riservatezza;

6. 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 di Parghelia 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; garantisce, 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;

7. Ai fini delle definizioni di cui al presente Regolamento si deve fare riferimento, al Regolamento UE 2016/679 (di seguito anche RGPD), al conseguente D.Lgs. 101/2018, al novellato D.Lgs. 196/2003 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali) ed al D.Lgs. 51/2018 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.

Art. 2-Definizioni

1) Ai fini del presente regolamento si intende:

- a) “**Codice**”, il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni ed integrazioni;
- b) “**impianto di videosorveglianza**”, qualunque impianto di ripresa, fissa o mobile, composto da una o più telecamere, in grado di riprendere e registrare immagini e suoni, utilizzato per le finalità indicate dall’articolo 3 del presente regolamento;
- c) “**sistema di Videosorveglianza**”, un sistema attraverso il quale si effettua la raccolta, la registrazione, la conservazione e in generale l’utilizzo di immagini e videoriprese relative a persone fisiche identificate o identificabili, anche indirettamente;
- d) “**sistema di Geolocalizzazione**”, un sistema attraverso il quale si effettua la raccolta, la registrazione, la conservazione e in generale l’utilizzo di informazioni sulla localizzazione geografica relative a persone fisiche identificate o identificabili, anche indirettamente;
- e) “**banca dati**”, il complesso di dati personali acquisiti mediante l’utilizzo degli impianti di videosorveglianza;
- f) “**trattamento**”, qualunque operazione o complesso di operazioni, svolti con l’ausilio dei 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 diffusione, la cancellazione e la distribuzione di dati personali;
- g) “**dato personale**”, qualunque informazione relativa a persona fisica, identificata o identificabile anche indirettamente e rilevata con trattamenti di immagini effettuati mediante gli impianti di videosorveglianza;
- h) “**titolare del trattamento**”, secondo l’art. 4 del RGPD è “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”. Nel contesto di questo Regolamento, il titolare è il Comune di Parghelia, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;
- i) “**responsabile della gestione tecnica degli impianti di videosorveglianza**”, la persona fisica, legata da rapporto di servizio al titolare e preposta dal medesimo all’installazione ed alla manutenzione degli impianti di videosorveglianza;
- j) “**incaricati**”, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile del trattamento dei dati personali;
- k) “**interessato**”, la persona fisica a cui si riferiscono i dati personali;
- l) “**comunicazione**”, il dare conoscenza dei dati personali ad uno o più soggetti determinati diversi dall’interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- m) “**diffusione**”, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- n) “**dato anonimo**”, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- o) “**blocco**”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
- p) “**RGPD**”, acronimo di “Regolamento Generale di Protezione dei Dati” - è il Regolamento UE 2016/679 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”;

- q) “**Supervisore**”, è il soggetto, designato dal Titolare, che sovrintende l'utilizzo di un sistema di gestione delle informazioni, coordinando le attività dei soggetti autorizzati al trattamento dei dati;
 - r) “**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;
 - s) “**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;
 - t) “**terzo**”, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
 - 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) “**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;
- 2) Per tutte le altre definizioni utilizzate in tale Regolamento si rimanda all'art. 4 del RGPD.

Art. 3-Norme di riferimento

- 1) Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto da:
- a) Provvedimento generale in materia di videosorveglianza in ambito pubblico e privato del 08 aprile 2010 del Garante della protezione dei dati personali (G.U. n. 99 del 29/04/2010);
 - b) Linee guida sulla Videosorveglianza negli enti locali dell'ANCI del 09 novembre 2010;
 - c) Circolare del Ministero dell'Interno inerente i Sistemi di videosorveglianza e relative specifiche tecniche per i Comuni del 02 marzo 2012 e successive indicazioni;
 - d) Regolamento UE Generale sulla Protezione dei Dati 2016/679 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” (anche “RGPD/GDPR”);
 - e) Decreto Legislativo 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali” come modificato ed integrato dal D.Lgs 101/2018;
 - f) Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018, pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018, inerente all'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto del Garante della protezione dei dati personali;
 - g) Direttiva UE 2016/680 relativa “alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”, recepita con il D.lgs. 51/2018;
 - h) riferimento agli articoli 7 del D.lgs. 51/2018 (sul trattamento di categorie particolari di dati personali), 6 c. 7 del D.L. 11/2009 (sulle Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori”) e 54 del D.lgs. 267/2000 (Testo Unico Enti Locali);

- i) DPR del 15/01/2018, n. 15, 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";
- j) Decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48, recante "Disposizioni urgenti in materia di sicurezza delle città" e successive modificazioni ed integrazioni del D.L. 14.06.19 n. 53_convertito con modifiche con L. 8 agosto 2019 n. 77.
- k) Linee guida 03/2019 v.2 del 29 gennaio 2020 pubblicate dall'EDPB, inerenti il trattamento di dati personali attraverso dispositivi video;
- l) Le regole per installare telecamere del 05 dicembre 2020 ed il vademecum e le FAQ in materia di videosorveglianza del 03 dicembre 2020 del Garante della protezione dei dati personali.

Art.4-Principi generali per il trattamento dei dati mediante sistema di videosorveglianza

1. Il presente regolamento garantisce che il trattamento dei dati personali, acquisiti mediante l'utilizzo degli impianti e sistemi di videosorveglianza, si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce al contempo il rispetto dei diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento;

2. Il trattamento dati viene acquisito dal sistema di videosorveglianza del Comune di Parghelia e potrebbe essere collegato alle centrali di controllo ubicate presso le sedi della Polizia Locale e delle altre Forze dell'Ordine, qualora dovessero essere attivate le opportune convenzioni/patti di sicurezza urbana "integrata";

3. Già con l'art. 6, commi 7 e 8, del cosiddetto "decreto sicurezza" approvato con Decreto-legge 23 febbraio 2009, n. 11 e convertito nella legge 23 aprile 2009, n. 38, denominato "Piano straordinario di controllo del territorio", è consentito, ai Comuni di far uso di sistemi di videosorveglianza al fine di prevenzione dei reati e controllo del territorio, mentre prima tali finalità non erano perseguibili in quanto di competenza delle autorità di polizia. Per i Comuni, quindi, non esiste più il limite della finalità delle riprese, ma è possibile che la videosorveglianza abbia uno scopo di semplice tutela del territorio, per cui è ammissibile a fini di controllo delle violazioni (ad esempio in materia di rifiuti). Ai sensi della vigente normativa in materia di sicurezza urbana, quindi, 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 D.L. 14/2017, convertito nella legge 18 aprile 2017 n. 48, all'art. 4, confermato nel D.L. del 14 giugno 2019 n. 53 convertito con modificazione con L. del 8 agosto 2019 n. 77 e meglio 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. Gli impianti di videosorveglianza installati o in corso di realizzazione dal Comune di Parghelia e, eventualmente, dai Comuni convenzionati per il servizio di Polizia Locale, attengono in via principale alla tutela della sicurezza urbana, alla tutela della sicurezza pubblica, alla tutela del patrimonio comunale, alla tutela della protezione civile e della salute, alla tutela della sicurezza stradale, alla tutela ambientale ed al presidio eventuale anche di ulteriori attività di polizia amministrativa, come il controllo sulla circolazione dei veicoli e la tutela ambientale;

4. Si riassumono di seguito i principi per la gestione dei sistemi / impianti e per il trattamento dei dati:

- a) **Principio di liceità** – Il trattamento di dati personali eseguito attraverso sistemi di videosorveglianza da parte di soggetti pubblici è consentito allorquando è necessario per

l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune ed il Titolare del trattamento in ossequio al disposto di cui all'art. 6, Paragrafo 1, le4. e), RGPD. Il trattamento dati è effettuato dal Comune di Rombio esclusivamente per lo svolgimento delle funzioni istituzionali;

- b) **Principio di necessità** - Sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. In ambito pubblico e con specifico riferimento alla necessità, è bene precisare che la rilevazione dei dati non potrà essere estesa ad ambiti, aree o attività che non presentino rischi concreti o non caratterizzate da esigenze di dissuasione e deterrenza. Allo stesso modo, laddove la finalità venga individuata nella protezione del bene o dei beni a fronte di atti di vandalismo, il posizionamento di sistemi di videosorveglianza potrà essere considerato lecito solo laddove sia stata valutata l'inefficacia di misure alternative e meno impattanti, quali ad esempio controlli da parte del personale di sicurezza, sistemi di allarme, misure di sicurezza apposte agli ingressi o autorizzazioni all'accesso fisico degli edifici;
- c) **Principio di proporzionalità** - Nella commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo qualora altre misure siano state preventivamente ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti (es. controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi). In ogni caso l'Ente garantisce che il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da controllare e/o proteggere;
- d) **Principio di finalità** – Gli scopi perseguiti devono essere determinati, espliciti e legittimi. È consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana, 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;

Art.5- Finalità dei sistemi

- 1) Le finalità di utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono conformi alle funzioni istituzionali attribuite al Comune di Parghelia. dalla legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Municipale, dalla legge regionale n. 15/2018, dallo statuto e dai regolamenti comunali, nonché dal decreto legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 "disposizioni urgenti in materia di sicurezza delle città" e successive modificazioni ed integrazioni e dalle altre disposizioni normative applicabili al Comune di Parghelia. 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 o protocolli operativi condivisi;
- 2) In particolare, l'uso di impianti di videosorveglianza è strumento per l'attuazione di un sistema integrato di politiche per la sicurezza urbana, di cui alle fonti normative sopra citate;
- 3) Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato ai fini di:
 - a) tutela della sicurezza urbana e della sicurezza pubblica;
 - b) tutela del patrimonio comunale;
 - c) tutela della protezione civile e della salute;
 - d) tutela della sicurezza stradale e controllo della circolazione dei veicoli;
 - e) tutela ambientale, contrasto all'abbandono dei rifiuti e polizia amministrativa;
 - f) supporto alle attività di protezione civile;
 - g) unicamente in qualità di polizia giudiziaria, prevenzione, indagine, accertamento e

- perseguimento di reati o esecuzione di sanzioni penali, nell'ambito di attività di P.G.;
- 4) Il sistema di videosorveglianza può comportare il trattamento di dati personali che possono essere rilevati da telecamere tradizionali ed eventualmente da varchi lettura targhe, in conformità alla DPIA.
 - 5) Le modalità di impiego dei dispositivi mobili saranno stabilite nel disciplinare approvato dalla Giunta Comunale e attuato con apposito provvedimento del Comando di Polizia Locale;
 - 6) Nel rispetto delle finalità previste dal presente Regolamento, l'Ente potrà promuovere politiche di controllo del territorio integrate con organi istituzionalmente preposti alla tutela della sicurezza e dell'ordine pubblico. Dette politiche di controllo integrato e/o di collaborazione con altri Corpi o Organi preposti alla tutela della sicurezza e dell'ordine pubblico, anche al fine di consentire la visualizzazione diretta delle immagini degli apparati di videosorveglianza, vengono previamente disciplinati con separati accordi in forma scritta.

CAPO 2- SOGGETTI COINVOLTI NEL TRATTAMENTO

Art.6- Soggetti

1) Per le immagini riprese e/o registrate nel Comune di Parghelia, il titolare dei dati è il Comune medesimo. A tal fine il Comune è rappresentato dal Sindaco, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza. Per le immagini riprese e/o registrate in altri Comuni, eventualmente convenzionati, il titolare dei dati è il Comune convenzionato;

Il Sindaco in qualità di rappresentante del titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza:

- a) definisce le linee organizzative per l'applicazione della normativa di settore;
 - b) individua e designa i soggetti autorizzati al trattamento dei dati acquisiti mediante l'utilizzo degli impianti di videosorveglianza, impartendo istruzioni ed assegnando compiti e responsabilità;
 - c) detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;
 - d) vigila sulla puntuale osservanza delle disposizioni impartite.
- 2) I Designati al trattamento dei dati rilevati con apparecchi di videosorveglianza sono:
- a) il Comandante del servizio di Polizia Locale per le telecamere collegate alla centrale operativa o gli agenti autorizzati dal Comandante della Polizia Locale;
 - b) gli altri dirigenti dei servizi competenti per le telecamere a tutela del patrimonio comunale o non collegate alla centrale operativa della polizia locale;
 - c) gli autorizzati alla gestione dell'impianto nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio e con specifici limiti di azione.

Tali designati vengono puntualmente individuati con atto del Comune titolare in relazione al trattamento delle immagini di propria competenza, così come definito nel paragrafo 1 del presente articolo, con cui impartire direttive e fornire indicazioni per la gestione ottimale della videosorveglianza. Possono essere individuati dal Comune per il proprio ambito di competenza ulteriori designati in ragione di necessità.

- 3) L'amministratore o gli amministratori di sistema sono designati dai Comuni per ambito di competenza. Nell'atto di designazione il Comune, in qualità di titolare del trattamento, può impartire direttive e fornire indicazioni per la gestione ottimale della videosorveglianza.
- 4) Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi;
- 5) A tutti i designati - previa specifica formazione - saranno distribuite idonee istruzioni;

6) Ai soggetti esterni al Comune e dei quali questo si avvale a qualsiasi titolo, in qualità di responsabili ex art. 28 del GDPR, per lo svolgimento di servizi e attività (esempio ditte per la manutenzione), per le quali si trattano dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento, si applicano le disposizioni previste dal Regolamento UE vigente. I rapporti con i Responsabili esterni, ex art. 28 del GDPR, sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri.

CAPO 3- TRATTAMENTO DEI DATI PERSONALI

Art.7- Modalità di raccolta e requisiti dei dati personali

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, consentono riprese video e possono essere dotate di brandeggio e di zoom ottico e sono collegate alla centrale operativa del Comando di Polizia Locale, che potrà visionarle esclusivamente per il perseguimento dei fini istituzionali:

- a) sulla base di denunce di atti criminosi da parte dei cittadini, per il successivo inoltro delle eventuali fonti di prova all'autorità giudiziaria;
- b) sulla base di segnalazioni relative ad atti criminosi accertate direttamente dagli organi di polizia in servizio sul territorio cittadino;
- c) sulla base di atti criminosi che vengono rilevati direttamente dagli operatori di polizia nel visionare le immagini trasmesse in diretta dalle telecamere, nell'esercizio delle proprie funzioni.
- d) sulla base di richieste specifiche per indagini da parte dell'autorità giudiziaria;
- e) sulla base di ogni altra richiesta di specifici organi/autorità che siano espressamente autorizzati, secondo specifiche norme di legge.

3) Le immagini videoregistrate sono conservate per il periodo indicato all'art. 8. Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione ove tecnicamente possibile - mediante sovra-registrazione, con modalità tali da rendere non più utilizzabili i dati cancellati.

Art.8- Trattamento e conservazione dei dati

1) I dati personali oggetto di trattamento effettuato con l'utilizzo degli impianti di videosorveglianza nel rispetto delle misure minime indicate dalla normativa relativa alla protezione delle persone fisiche sono:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per le finalità di cui all'articolo 5 del presente regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;
- c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- d) conservati per le telecamere collegate alla centrale operativa del Comando di Polizia Locale per un periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione, che possono essere estesi fino a 90 giorni tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati, con particolare riferimento ai varchi lettura targhe e previa segmentazione degli accessi da effettuare in relazione a specifiche ed evidenti esigenze investigative e di polizia giudiziaria nonché specifiche richieste da parte dell'Autorità prefettizia e giudiziaria, tenuto conto di eventuali ulteriori necessità di conservazione in caso di ricorsi. Termini puntuali di conservazione dei dati degli utenti in relazione alle varie finalità saranno individuati nel disciplinare - programma di cui all'art. 34 del presente regolamento;

- e) conservati per le telecamere a tutela del solo patrimonio comunale (o per altre telecamere non collegate alla centrale operativa del Corpo di Polizia Locale) per un periodo non superiore a 72 ore successive alla rilevazione, fatte salve speciali e diverse esigenze debitamente documentate.
- 2) Ogni decisione volta alla conservazione dei dati per un periodo più esteso rispetto a quello indicato dovrà essere ampiamente giustificata tramite idonea documentazione comprovante le ragioni di detta esigenza.

Art.9- Informativa

- 1) I soggetti interessati che stanno per accedere o che si trovano in una zona videosorvegliata, devono essere sempre informati mediante appositi cartelli, nei casi specificatamente previsti dalla normativa vigente.
- 2) A tal fine, il Garante della Privacy, con il provvedimento in materia di videosorveglianza - 8 aprile 2010 confermato poi con il provvedimento del 5 dicembre 2020 con il quale ha pubblicato "Le linee guida per installare le telecamere" ed allegato le Faq messe a punto dal Garante per la protezione dei dati personali sulle questioni concernenti il trattamento dei dati personali nell'ambito dell'installazione di impianti di videosorveglianza da parte di soggetti pubblici e privati, ha ritenuto che l'informativa può essere fornita utilizzando un modello semplificato, che deve contenere, tra le altre informazioni, le indicazioni sul titolare del trattamento e sulla finalità perseguita (conformi a quanto previsto dall'EDPB nelle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video – adottate il 29 gennaio 2020);
3) Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli.
- 4) Il supporto con l'informativa minima:
 - a) deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
 - b) deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
 - c) l'informativa deve rinviare a un testo completo contenente tutti gli elementi di cui all'art. 13 del RGPD, indicando come e dove trovarlo (ad es. sul sito Internet del titolare del trattamento o affisso in bacheche o locali dello stesso).
- 5) In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, possono essere installati più cartelli;
- 6) L'informativa di cui sopra non è dovuta nel caso di utilizzo di telecamere a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati;
- 7) L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere.

Art.10 – Comunicazione e diffusione dei dati personali a Enti o Organismi pubblici

- 1) La comunicazione dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento, da parte del Comune di Parghelia a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento;
- 2) Ai sensi e per gli effetti del comma 1 del presente articolo, non si considera comunicazione la

conoscenza dei dati personali da parte dei soggetti incaricati ed autorizzati per iscritto a compiere operazioni di trattamento dal titolare o dai responsabili e che operano sotto la loro diretta autorità;

- 3) È in ogni caso fatta salva la comunicazione o diffusione di dati personali richiesti, in conformità alla legge, da forze di polizia, Autorità Giudiziaria, organismi di informazione e sicurezza, o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, del Codice, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Art.11 – Utilizzo di particolari sistemi

- 1) Il sistema di videosorveglianza in uso al Comando di Polizia Locale di Parghelia comprende apparecchi quali:
 - a) **fototrappole e sistemi mobili di videosorveglianza** da posizionare in località difficilmente accessibili o sorvegliabili, al solo titolo esemplificativo zone di campagna, strade interpoderali o aree urbane oggetto di degrado. La finalità dell'utilizzo di tali sistemi di controllo è quella di monitorare le aree oggetto di deturpazione da parte dell'utenza laddove non è possibile farlo diversamente, ai fini sia dell'accertamento delle eventuali violazioni amministrative o penali, sia ai fini della deterrenza alla prosecuzione di azioni di degrado da parte della cittadinanza e dell'utenza di passaggi. In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza fissi e/o mobili, **ancorché temporaneamente occultati**, risulta consentito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree **segnalate** come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo tradizionali. Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure, nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, legge 24 novembre 1981, n. 689).
 - b) **apparecchi, per l'accertamento delle violazioni delle norme di comportamento del Codice della Strada**, che consentono la determinazione dell'illecito in tempo successivo, poiché il veicolo oggetto del rilievo è a distanza dal posto di accertamento o comunque nell'impossibilità di essere fermato in tempo utile o nei modi regolamentari, siano esse in postazione fisse o mobili, in presenza o meno dell'operatore. I sistemi elettronici di rilevamento delle infrazioni inerenti violazioni del codice della strada vanno obbligatoriamente segnalate da cartello/informativa anche in base alla disciplina di settore. L'utilizzo di tali sistemi è lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese. La ripresa del veicolo non deve comprendere (o deve mascherare), per quanto possibile, la parte del video o della fotografia riguardante soggetti non coinvolti nell'accertamento amministrativo (es. eventuali pedoni o altri utenti della strada). Le fotografie o i video che attestano l'infrazione non devono essere inviati al domicilio dell'intestatario del veicolo, ma l'interessato, ossia la persona eventualmente ritratta nelle immagini, può richiederne copia oppure esercitare il diritto di accesso ai propri dati (fermo restando che dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo);
 - c) **Sistemi di controllo accessi ZTL e lettura targhe**: L'istituzione della Zona a Traffico Limitato è finalizzata alla preminente salvaguardia del territorio comunale, ponendosi come strumento indispensabile per il bilanciamento tra il diritto alla mobilità e la tutela della salute pubblica, dell'ambiente e del patrimonio storico. Al fine di garantire l'efficacia del provvedimento, il controllo degli accessi è demandato a un sistema di rilevazione automatica (varchi elettronici), debitamente omologato e autorizzato dal Ministero delle Infrastrutture e dei Trasporti ai sensi dell'art. 7 del D.Lgs. 285/1992 e del D.P.R. 250/1999. Tale sistema è preordinato all'accertamento delle infrazioni in modo imparziale e continuativo, assicurando la fluidità della circolazione e la protezione delle aree pedonali. Il

trattamento dei dati personali e delle immagini acquisite mediante i dispositivi video avviene nel rigoroso rispetto del Regolamento UE 2016/679 (GDPR) e delle disposizioni del Garante per la Protezione dei Dati Personali; le immagini vengono rilevate solo in caso di accertata violazione, con modalità che garantiscono la pertinenza e la non eccedenza dei dati raccolti. La conservazione delle registrazioni è limitata al tempo strettamente necessario per la contestazione dell'infrazione e la gestione di eventuali ricorsi, previa apposizione di idonea segnaletica informativa che avvisi l'utenza dell'inizio della zona videosorvegliata, garantendo così trasparenza e sicurezza a tutti i cittadini.

- 2) Gli apparati di videosorveglianza modulare riposizionabili vengono installati secondo necessità, nei luoghi teatro di illeciti penali; possono essere utilizzati per accertare illeciti amministrativi, solo qualora non siano altrimenti accertabili con le ordinarie metodologie di indagine e non si possa fare ricorso a strumenti e sistemi di controllo alternativi e nel rispetto del principio di minimizzazione;
- 3) Il trattamento dei dati personali effettuati con simili sistemi di ripresa deve rispettare i principi di cui all'art. 5 del Regolamento UE 2016/679 ed in particolare i dati personali oggetto di trattamento debbono essere adeguati, pertinenti, e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati.

Art. - 12. Strumenti diversi di rilevazione immagini: body cam e dash cam

1. Gli operatori di Polizia Locale possono utilizzare, per i servizi a maggior rischio operativo, delle body cam (telecamere installate sul corpo dell'operatore in servizio) e delle dash cam (telecamere a bordo dei veicoli di servizio) in conformità alle indicazioni dettate dal Garante della Privacy con nota del 30/9/2014, con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi il cui trattamento dei dati è ricondotto nell'ambito del D.Lgs. 51/2018 trattandosi di "dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela all'ordine e della sicurezza pubblica, nonché di polizia giudiziaria".
2. Il Comando di Polizia Locale curerà la predisposizione di uno specifico disciplinare tecnico interno, da somministrare agli operatori di Polizia Locale che saranno dotati di microcamere, con specificazione dei casi in cui le microcamere stesse devono essere attivate, dei soggetti autorizzati a disporre l'attivazione, delle operazioni autorizzate in caso di emergenza e di ogni altra misura organizzativa e tecnologica necessaria alla corretta e legittima gestione di detti dispositivi e dei dati trattati.
3. Le videocamere e le schede di memoria di cui sono dotati i sistemi di cui al comma 1 dovranno essere contraddistinte da un numero seriale che dovrà essere annotato in apposito registro recante il giorno, l'orario, i dati indicativi del servizio e la qualifica e nominativo del dipendente che firmerà la presa in carico e la restituzione. La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato. Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza delle situazioni descritte al comma 1.
4. Il trattamento dei dati personali effettuati con simili sistemi di ripresa devono rispettare i principi del Codice Privacy richiamati nel presente regolamento ed in particolare i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati.

Art.13 – Utilizzo di sistemi aeromobili a pilotaggio remoto (UAS/DRONI)

1. Il Comune può utilizzare sistemi aeromobili a pilotaggio remoto (UAS – Unmanned Aircraft Systems), comunemente denominati “droni”, nell’ambito del sistema comunale di videosorveglianza esclusivamente per finalità istituzionali di interesse pubblico, nel rispetto della normativa europea e nazionale vigente in materia aeronautica, di protezione dei dati personali e di sicurezza urbana.
2. L’utilizzo degli UAS è consentito esclusivamente per:
 - a) tutela della sicurezza urbana e dell’incolumità pubblica;
 - b) monitoraggio del territorio comunale;
 - c) protezione civile e gestione delle emergenze;
 - d) prevenzione e accertamento di illeciti ambientali;
 - e) contrasto all’abbandono di rifiuti;
 - f) monitoraggio di incendi, dissesti e situazioni di pericolo;
 - g) verifica di abusi edilizi;
 - h) controllo della viabilità e supporto operativo alla Polizia Locale;
 - i) monitoraggio di aree difficilmente accessibili o particolarmente estese.
3. L’impiego degli UAS deve avvenire nel rispetto dei principi di liceità, necessità, proporzionalità, minimizzazione dei dati e limitazione delle finalità previsti dal Regolamento (UE) 2016/679 (GDPR).
4. È vietato l’utilizzo dei droni per:
 - a) forme di controllo generalizzato della popolazione;
 - b) sorveglianza sistematica e indiscriminata delle persone;
 - c) monitoraggio continuativo di comportamenti individuali;
 - d) riprese eccedenti rispetto alle finalità istituzionali perseguite;
 - e) riprese di aree private non pertinenti;
 - f) utilizzo di sistemi biometrici o di riconoscimento facciale, salvo specifica previsione normativa.
5. Le operazioni di volo devono essere motivate da specifiche esigenze operative e devono essere effettuate esclusivamente quando le finalità perseguite non possano essere efficacemente raggiunte mediante strumenti meno invasivi.
6. L’utilizzo degli UAS deve avvenire nel rispetto del Regolamento (UE) 2018/1139, del Regolamento di esecuzione (UE) 2019/947, del Codice della Navigazione, della normativa ENAC vigente e delle ulteriori disposizioni applicabili.
7. Qualora le operazioni comportino il superamento dei limiti previsti per la categoria “open” delle operazioni UAS, il Comune o il Corpo di Polizia Locale provvedono preventivamente:
 - a) alla valutazione del rischio operativo;
 - b) all’adozione delle misure di mitigazione del rischio;
 - c) all’ottenimento delle autorizzazioni previste dalla normativa vigente e da ENAC.
8. L’impiego degli UAS da parte della Polizia Locale per finalità istituzionali è subordinato agli eventuali provvedimenti autorizzativi previsti dalla normativa statale e aeronautica vigente, compreso, ove necessario, il riconoscimento quale aeromobile di Stato ai sensi dell’art. 746 del Codice della Navigazione.
9. Le operazioni di pilotaggio e il trattamento dei dati acquisiti possono essere effettuati esclusivamente da personale autorizzato, adeguatamente formato e in possesso delle eventuali abilitazioni richieste dalla normativa vigente.
10. I dati personali raccolti mediante UAS sono trattati nel rispetto del GDPR, del D.Lgs. 196/2003 e del D.Lgs. 51/2018, limitatamente alle finalità istituzionali perseguite.
11. L’utilizzo degli UAS comportante trattamenti suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone fisiche è subordinato allo svolgimento della Valutazione d’Impatto sulla Protezione dei Dati (DPIA) ai sensi dell’art. 35 del GDPR e, nei casi previsti dalla legge, alla preventiva consultazione del Garante per la protezione dei dati personali.
12. Le immagini e i dati acquisiti mediante UAS sono conservati per il tempo strettamente necessario al perseguimento delle finalità istituzionali e comunque nel rispetto dei termini previsti dal presente regolamento per il sistema di videosorveglianza comunale, fatti salvi eventuali ulteriori obblighi di conservazione connessi ad attività di polizia giudiziaria o procedimenti amministrativi e giudiziari.
13. Restano ferme le disposizioni del presente regolamento in materia di sicurezza dei dati, accessi autorizzati, tracciabilità delle operazioni e diritti degli interessati.

Art.14 – Cessazione del trattamento dei dati personali

- 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'art 2 del D. Lgs. 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.

Art.15 – 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 ex art. D. Lgs 51/2018:
 - 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 ex art. 13 RGPD e art. 10 e ss. D. Lgs. 51/2018;
 - c) di ottenere:
 - i) la conferma dell'esistenza o meno di dati personali che lo riguardano;
 - ii) la trasmissione in forma intelligibile dei medesimi dati e della loro origine;
 - iii) la cancellazione nei casi previsti dal Regolamento UE 2016/679 qualora sussista uno dei motivi di cui all'art. 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;
 - b) 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'art. 21 del Regolamento UE 2016/679. Il designato informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti;
 - a. di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle ipotesi specificate all'art. 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;
 - c) L'istanza per l'esercizio dei diritti dell'interessato è presentata al titolare o al designato al trattamento dati. È considerata sempre l'opportunità di coinvolgere il Responsabile della Protezione Dati;
 - d) Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare le informazioni utili alla sua identificazione tramite il sistema di videosorveglianza, fra cui il luogo, la data e la fascia oraria della possibile ripresa. Il designato accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della loro acquisizione, in ossequio alla previsione di cui all'art. 15, paragrafo 4 del Regolamento UE 2016/679;
 - e) Qualora non sia possibile identificare l'interessato (o in caso di richieste eccessive o manifestamente infondate) il designato – previa adeguata motivazione ed entro i termini

- di 7 giorni dalla richiesta – informerà l'interessato dell'impossibilità di dare seguito alla richiesta;
- f) Per ciascuna delle richieste di accesso può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, secondo le modalità previste dalla normativa vigente.

Art.16 – Accesso ai filmati

- 1) Chiunque ritenga di essere stato ripreso dai dispositivi di controllo e videosorveglianza gestiti dall'Ente può esercitare il diritto di accesso ai propri dati personali ai sensi dell'art. 15 del Regolamento UE 2016/679 (GDPR). L'estrazione di copia è consentita solo laddove non si pregiudichi la riservatezza di soggetti terzi. In presenza di dati di terzi, il rilascio di copia è subordinato alla previa anonimizzazione dei dati a cura e spese del richiedente, che verranno stabiliti dal Regolamento sul Diritto di accesso. Qualora la copia richieda operazioni di anonimizzazione non effettuabili con la strumentazione in dotazione all'Ente, quest'ultimo potrà avvalersi di ditte esterne specializzate; in tal caso, il preventivo della ditta verrà sottoposto al richiedente che dovrà saldarlo integralmente prima della lavorazione;
- 2) Al di fuori dei diritti dell'interessato, di cui all'articolo precedente del presente regolamento, l'accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente, come riportati all'art. 7 punto 2 del presente regolamento;
- 3) Ordinariamente ogni richiesta dovrà essere specifica, formulata per iscritto, motivata ed indirizzata al designato del trattamento dei dati competente (o al Comando di Polizia Locale formalmente designato) entro il periodo previsto dal presente Regolamento per la conservazione dei dati e deve contenere i dati anagrafici e copia del documento di identità del richiedente, l'indicazione puntuale e circoscritta del luogo, della data e della fascia oraria (con uno scarto non superiore a 30 minuti) in cui si ritiene di essere stati ripresi, eventuali elementi utili al riconoscimento (es. modello e targa del veicolo, colore e tipologia degli indumenti indossati).
- 4) Per finalità di indagine, l'Autorità Giudiziaria e la polizia giudiziaria possono acquisire copia delle riprese in formato digitale, formulando specifica richiesta scritta.
- 5) È consentito all'Autorità Giudiziaria ed alla Polizia Giudiziaria di acquisire copia delle immagini. Occorre peraltro ricordare che le qualifiche possedute dagli appartenenti alla Polizia Locale riguardano la polizia stradale, la polizia amministrativa, la polizia giudiziaria e la sicurezza pubblica con finalità di ausilio alle Forze di Polizia ex Legge nr. 121/1981 (cfr. Legge Quadro sul l'ordinamento della polizia municipale nr. 65/1986);
- 6) Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, i filmati possono essere richiesti ed acquisiti dall'organo di polizia stradale che ha proceduto ai rilievi ed in capo al quale è l'istruttoria relativa all'incidente;
- 7) Fermi restando i poteri di acquisizione d'ufficio degli organi di Polizia Stradale di cui al comma precedente, i soggetti coinvolti in un sinistro stradale (o i loro legali rappresentanti muniti di procura) possono presentare istanza di accesso ai filmati per la tutela dei propri diritti in sede civile o penale, secondo le seguenti modalità: Il rilascio di copia dei filmati su supporto digitale è consentito solo laddove non risultino visibili soggetti terzi o dati personali non pertinenti al sinistro. Qualora tali dati siano presenti, il rilascio della copia è subordinato alla preventiva anonimizzazione (oscuramento) dei volti e delle targhe estranee a cura dell'Ente.
- 8) L'accesso può essere negato o differito qualora sussista un pregiudizio per attività di indagine

penale in corso o su disposizione dell'Autorità Giudiziaria.

- 9) L'accesso ai dati della videosorveglianza è disciplinato dalle disposizioni del Regolamento UE 2016/679 (GDPR) per quanto concerne la tutela dei dati personali, e dalla Legge 241/1990 per quanto concerne l'accesso ai documenti amministrativi necessari alla tutela di un interesse giuridicamente rilevante.
- 10) In caso di fatti penalmente rilevanti, l'estrazione dei dati è consentita all'Autorità Giudiziaria e alla Polizia Giudiziaria, secondo le modalità previste dal Codice di Procedura Penale. Il cittadino vittima di un reato, al fine di esercitare il proprio diritto di difesa e nelle more della formalizzazione della denuncia/querela, ha facoltà di:
 - a) Richiedere la conservazione (congelamento) dei dati: Presentando istanza scritta entro i termini di conservazione ordinaria. L'Ente assicura la conservazione delle immagini per un periodo di 90 giorni, decorso il quale, in assenza di acquisizione da parte della Polizia Giudiziaria, i dati verranno definitivamente cancellati.
 - b) Esercitare il diritto di visione: Previa istanza motivata, il cittadino può visionare le immagini presso gli uffici dell'Ente al solo scopo di confermare la rilevanza dell'evento o identificare elementi utili alla denuncia. È vietata l'estrazione di copia o la ripresa con dispositivi propri.

Nell'ambito delle investigazioni difensive (ai sensi dell'Art. 391-quater c.p.p.), il difensore della persona offesa o della persona sottoposta alle indagini può richiedere copia dei filmati su supporto digitale. L'istanza deve specificare i fatti per cui si procede e la stretta pertinenza delle immagini con l'attività difensiva. Il rilascio è subordinato al rimborso delle spese tecniche di estrazione e all'eventuale anonimizzazione di terzi estranei ai fatti. L'Ente si riserva di negare l'accesso diretto o il rilascio di copia qualora sussista il rischio di pregiudizio per le indagini o qualora sia già intervenuto un sequestro delle immagini da parte dell'Autorità Giudiziaria.

- 11) Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'Art. 391-quater c.p.p., può richiedere copia digitale dei filmati della videosorveglianza presentando specifica richiesta al designato del trattamento dei dati, previo il pagamento delle relative spese;
- 12) Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al designato del trattamento dati che i filmati siano conservati oltre i termini di Legge, per essere messi a disposizione dell'organo di polizia procedente. La richiesta deve comunque pervenire entro i termini di conservazione previsti. Spetta all'Organo di polizia in questione procedere a presentare formale richiesta di acquisizione dei filmati. Tale richiesta dovrà comunque pervenire entro tre mesi dalla data dell'evento, decorsi i quali i dati non saranno ulteriormente conservati;
- 13) In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dal designato del trattamento dei dati deve lasciare traccia delle operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, in modo da garantire la genuinità dei dati stessi;
- 14) Salvo l'ipotesi di conservazione per diverse finalità, i dati si intendono disponibili per i normali tempi di conservazione.

Art.17 – Valutazione di impatto sulla protezione dei dati

- 1) In ossequio al disposto di cui all'art. 35 Regolamento UE 2016/679, qualora il trattamento di dati realizzato mediante i sistemi oggetto del presente regolamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare provvederà, previa consultazione con il Responsabile della Protezione dei Dati, all'effettuazione di una valutazione di impatto sulla protezione dei dati personali. Il Titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei

dati a norma dell'articolo 35 indichi che il trattamento potrebbe rappresentare un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;

- 2) La valutazione di impatto non verrà effettuata qualora il trattamento dovesse rientrare nell'elenco delle tipologie di trattamenti, redatto dal Garante della Privacy (Allegato 1 al Provvedimento n. 467 dell'11 Ottobre 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto), per le quali non è richiesta.

Art.18 – Utilizzo in ambiente di lavoro

- 1) Ai sensi di quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300, gli impianti di videosorveglianza e gli strumenti di rilevazione di dati di geolocalizzazione non possono essere utilizzati per effettuare controlli sull'attività lavorativa dei dipendenti dell'ente, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati; L'installazione è lecita solo per: esigenze organizzative e produttive, sicurezza del lavoro (es. monitoraggio aree pericolose), tutela del patrimonio aziendale/comunale (es. prevenzione furti o vandalismi).
- 2) Qualsiasi utilizzo di sistemi in ambienti di lavoro deve soddisfare i principi di liceità, non eccedenza e proporzionalità. Il requisito di liceità del trattamento, previsto dal Garante della protezione dati, è il rispetto delle altre garanzie previste dalla normativa di settore in materia di installazione di impianti audiovisivi e altri strumenti di controllo (art. 4 della l. 300/1970);
- 3) Il titolare deve quindi attivarsi, in caso di necessità, per l'attuazione di misure di garanzia ai sensi dello Statuto dei Lavoratori.

CAPO 4- MISURE DI SICUREZZA

SICUREZZA DEI SISTEMI DI VIDEOSORVEGLIANZA, ACCOUNTABILITY E GESTIONE DEL RISCHIO

Art. _19 – Principi generali di sicurezza del trattamento

1. Tutti i sistemi di videosorveglianza utilizzati dal Comune, inclusi impianti fissi, fototrappole, sistemi aeromobili a pilotaggio remoto (UAS/droni), dispositivi indossabili (body cam) e ogni altra tecnologia di acquisizione immagini e dati, devono garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del Regolamento (UE) 2016/679 (GDPR).

2. La sicurezza del trattamento costituisce requisito essenziale di legittimità dell'intero sistema di videosorveglianza comunale.

Art. 20 – Misure tecniche e organizzative minime

1. I sistemi adottati devono garantire congiuntamente:

- * la cifratura e, ove applicabile, la pseudonimizzazione dei dati personali;
- * la riservatezza, integrità, disponibilità e resilienza dei sistemi;
- * la protezione da accessi non autorizzati;
- * la tracciabilità delle operazioni effettuate sui dati;
- * la capacità di ripristino tempestivo dei dati in caso di incidente fisico o tecnico;
- * la verifica periodica dell'efficacia delle misure tecniche e organizzative.

1. Le misure di sicurezza devono essere proporzionate alla natura, al contesto e alle finalità del

trattamento, nonché al rischio per i diritti e le libertà degli interessati.

Art. 21 – Gestione del rischio e valutazione preventiva

1. L'introduzione o modifica di sistemi di videosorveglianza è subordinata a una preventiva valutazione del rischio, documentata nell'ambito della Valutazione d'Impatto sulla Protezione dei Dati (DPIA), ove prevista.
2. La DPIA è aggiornata periodicamente e comunque ogniqualvolta intervengano modifiche sostanziali nei sistemi, nelle finalità o nelle modalità di trattamento.
3. L'adeguatezza delle misure di sicurezza è oggetto di riesame periodico da parte del titolare del trattamento.

Art. 22 – Architettura dei sistemi e conservazione dei dati

1. I sistemi di videosorveglianza devono essere progettati privilegiando, ove tecnicamente possibile, soluzioni centralizzate e sicure per la gestione e conservazione dei dati.
2. La conservazione locale su dispositivi mobili o periferici è ammessa solo se adeguatamente protetta mediante sistemi di cifratura e misure idonee a prevenire perdita, sottrazione o alterazione dei dati.
3. I sistemi devono garantire la continuità operativa e la resilienza anche in caso di eventi accidentali o dolosi.

Art. 23 – Data breach e gestione delle violazioni di sicurezza

1. Per violazione dei dati personali ("data breach") si intende qualsiasi evento che comporti distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato ai dati trattati.
2. In caso di violazione dei dati, il Comune attiva senza indugio le procedure previste dalla normativa vigente e, in particolare:
 - a) notifica al Garante per la protezione dei dati personali nei termini di legge;
 - b) documentazione interna dell'evento;
 - c) valutazione del rischio per i diritti e le libertà degli interessati;
 - d) adozione di misure correttive e di contenimento.
3. Ove la violazione presenti un rischio elevato per gli interessati, il Comune provvede anche alla relativa comunicazione agli stessi, nei casi previsti dalla normativa.

Art. 24 – Responsabilità del titolare del trattamento

1. Il Comune, quale titolare del trattamento, è responsabile della conformità dei sistemi di videosorveglianza ai principi di sicurezza, integrità e riservatezza dei dati.
2. L'utilizzo di sistemi non conformi ai requisiti di sicurezza previsti dalla normativa vigente determina l'illegittimità del trattamento e l'inutilizzabilità dei dati acquisiti.
3. Il titolare del trattamento garantisce la verifica preventiva e periodica della conformità tecnica e organizzativa dei sistemi utilizzati.

Art. 25 – Integrazione con i sistemi speciali di videosorveglianza

1. Le disposizioni del presente Capo si applicano in modo trasversale a tutte le tecnologie disciplinate dal Regolamento comunale di videosorveglianza, incluse:

- * telecamere fisse e mobili;
- * fototrappole;
- * sistemi UAS/droni;
- * body cam;
- * eventuali ulteriori sistemi tecnologici evoluti.

1. Ogni sistema deve essere integrato nel complessivo assetto di sicurezza e governance dei dati del Comune.

Art.26 – Sicurezza dei dati personali

- 1) Ai sensi di quanto previsto dall'articolo 32 del Regolamento UE 2016/679, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono protetti da misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di cui al presente regolamento;
- 2) I dati personali oggetto di trattamento sono conservati presso la sala di controllo del Comando di Polizia Locale di Parghelia, alla quale può accedere il solo personale autorizzato secondo istruzioni che devono essere impartite in forma scritta dal designato del trattamento dei dati;
- 3) 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, aventi qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 57 del codice di procedura penale;
- 4) Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali profilazioni per l'utilizzo dei sistemi in base alle differenti dislocazioni territoriali degli stessi e le diverse funzioni in ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento;
- 5) Gli autorizzati al trattamento e i preposti sono dotati di proprie credenziali di autenticazione di accesso al sistema. Il sistema dovrà essere fornito di "log" di accesso.

Art.27 – Accesso alle centrali di controllo

- 1) I dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento, sono custoditi presso il Server ubicato presso il Comune di Parghelia, o eventualmente presso le altre sedi collegate specificate nel presente regolamento;
- 2) L'accesso alla sala di controllo è consentito solamente al personale in servizio della Polizia Locale autorizzato per iscritto, dal Comandante e agli incaricati addetti ai servizi, di cui ai successivi articoli.
- 3) Possono essere autorizzati solo incaricati di servizi rientranti nei compiti istituzionali dell'Ente o Organismo di appartenenza e per scopi connessi alle finalità di cui al presente regolamento, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali, preventivamente individuato dal titolare o dal designato al trattamento;
- 4) L'accesso da parte di soggetti diversi da quelli indicati ai commi precedenti del presente articolo è subordinato al rilascio, da parte del titolare, di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso. L'accesso

avviene in presenza di incaricati del Comune di Parghelia, individuati ai sensi del presente regolamento;

- 5) Gli incaricati vigilano sul puntuale rispetto delle istruzioni impartite dal Titolare e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art.28 – Accesso logico ai sistemi e ai dati.

- 1) L'accesso ai sistemi che gestiscono i dati oggetto del presente regolamento ed ai dati oggetto dello specifico trattamento, può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate su disposizione del designato del trattamento come individuato all'art. 6;
- 2) L'accesso ai sistemi di registrazione prevede l'adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei designati da parte del titolare, comunque non inferiore a sei mesi;
- 3) L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il perseguimento delle finalità definite per lo specifico trattamento di dati.

Art.29 – Sicurezza nelle trasmissioni

Il Titolare è tenuto a disporre l'adozione di adeguati sistemi di sicurezza per garantire la riservatezza delle trasmissioni telematiche nei contesti di propria competenza e responsabilità.

Art.30 – Utilizzo degli strumenti e dei supporti di memorizzazione

1. Gli strumenti assegnati che consentano l'accesso ai dati devono essere protetti da sistemi di autenticazione e non devono essere lasciati incustoditi;
2. Qualora la presa in carico delle immagini e delle videoriprese venga effettuata tramite riversamento dai supporti di memoria presenti negli strumenti di acquisizione, i file contenenti dati devono essere rimossi dai supporti una volta acquisiti i dati;
3. In caso di dismissione di supporti di memorizzazione, questi devono essere resi inutilizzabili tramite danneggiamento fisico irreparabile, in modo che non sia consentito in alcun modo il recupero dei dati trattati.

Art. 31 – Accesso ai dati da parte delle Forze di polizia e Autorità Giudiziaria

L'accesso alle immagini e ai dati registrati dai sistemi di videosorveglianza è consentito:

all'Autorità Giudiziaria, alla Polizia Giudiziaria, a tutte le Forze dell'Ordine, esclusivamente per finalità istituzionali connesse: alla prevenzione, all'accertamento, all'investigazione, alla repressione dei reati, alla tutela della sicurezza pubblica.

Le richieste devono essere motivate, formulate per iscritto, salvo casi di urgenza e riferite a specifici eventi, luoghi e fasce temporali. L'estrazione e la consegna delle registrazioni sono effettuate esclusivamente da personale autorizzato, devono essere tracciate, devono essere annotate in apposito registro degli accessi e delle estrazioni.

È vietato l'accesso indiscriminato o generalizzato ai sistemi di videosorveglianza comunali, salvo specifiche convenzioni o disposizioni normative. La trasmissione dei dati deve avvenire

mediante modalità idonee a garantire: sicurezza, integrità, riservatezza e tracciabilità del trattamento.

CAPO 5- TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art.32 – Tutela

- 1) Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 77 e seguenti del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e dagli artt. 37 e seguenti del D.Lgs. 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;
- 2) In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il Designato al trattamento dei dati personali, così come individuato dal precedente art. 6.

CAPO 6- ALTRE DISPOSIZIONI

Art.33 – Diritto al risarcimento, responsabilità e danno cagionati per effetto del trattamento dei dati personali

- 1) Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento ai sensi delle disposizioni di cui all'art. 82 del RGPD;
- 2) Il Titolare e/o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile;
- 3) Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2 del RGPD.

Art.34 – Provvedimenti attuativi

- 1) La Giunta comunale, sulla base degli indirizzi e principi contenuti nel presente regolamento, con propria deliberazione, adotta il "disciplinare - programma per l'utilizzo degli impianti di videosorveglianza". Il disciplinare - programma contiene regole più specifiche per l'utilizzo e la gestione del sistema di videosorveglianza e riporta tutte le misure di tipo fisico, tecnico ed organizzativo adottate; può individuare qualsiasi altro dettaglio, specificazione, regolamentazione della videosorveglianza nel rispetto del presente regolamento.
- 2) Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi derivanti dal presente Regolamento, fra cui l'adozione di atti che descrivano i trattamenti di dati effettuati dal titolare, che prevedano, coerentemente con le previsioni di cui al presente regolamento, in termini generali quanto segue:
 - a) le motivazioni dell'installazione dell'impianto;
 - b) la sintetica descrizione del trattamento e del flusso informativo;
 - c) l'architettura tecnologica dei sistemi di gestione dei dati;
 - d) le misure di sicurezza adottate;
 - e) l'eventuale necessità di effettuare una valutazione di impatto sulla protezione dei dati e l'esito;

- f) le categorie di destinatari a cui vengono comunicati i dati;
 - g) le modalità di comunicazione delle informazioni relative ai sistemi utilizzati nonché la definizione di ogni ulteriore e specifico elemento ritenuto utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento.
- 3) Spetta invece ai supervisori l'adozione di appositi atti che prevedano:
- a) l'autorizzazione ai soggetti che tratteranno i dati, specificando per ognuno il perimetro di azione;
 - b) la designazione dei responsabili del trattamento ai sensi dell'art. 28 RGPD che tratteranno i dati in nome e per conto del titolare;
 - c) la designazione degli Amministratori di Sistema, con specificazione degli ambiti di operatività;
 - d) l'elenco dei siti in cui potranno essere collocati i sistemi di acquisizione delle immagini e la tipologia delle forniture, sulla base delle necessità rilevate ed in osservanza al principio di proporzionalità;
 - e) l'attuazione di tutte le misure che garantiscano la sicurezza dei dati trattati e dei sistemi implementati.

Art.35 – Modifiche regolamentari

- 1) I contenuti del presente regolamento dovranno essere aggiornati nei casi di revisione normativa in materia di trattamento dei dati personali e in materia di videosorveglianza da parte del Consiglio Comunale.
- 2) In ogni caso, ogni modifica del presente regolamento dovrà essere effettuata tramite Consiglio Comunale.

Art.36 – Entrata in vigore

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

Art.37 – Norma di rinvio

- 1) Per quanto non disciplinato dal presente Regolamento si rinvia al D. Lgs. 101/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, che modifica il Codice Privacy di cui al D. Lgs. 196/2003 e al D. Lgs. 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, nonché ai provvedimenti generali sulla videosorveglianza approvati dall'Autorità garante per la protezione dei dati personali e alle indicazioni centrali dell'Anci e del Ministero dell'Interno.

**COMUNE DI PARGHELIA
(Provincia di Vibo Valentia)**

Allegato alla deliberazione di Consiglio Comunale n. 10 del 25/05/2026

OGGETTO: APPROVAZIONE REGOLAMENTO PER LA VIDEOSORVEGLIANZA E PER L'UTILIZZO DEI SISTEMI DI CONTROLLO DEL TERRITORIO.

=====

Parere di Regolarità Tecnica

Sulla presente proposta di deliberazione, ai sensi dell'art 49 comma 1 del D.Lgs. 267/2000 , si esprime in ordine alla regolarità tecnica della stessa **PARERE FAVOREVOLE**

**Il Responsabile del Servizio
Antonio LANDRO**





COMUNE DI PARGHELIA
(Provincia di Vibo Valentia)

OGGETTO: APPROVAZIONE REGOLAMENTO PER LA DISCIPLINA ED UTILIZZO DEGLI IMPIANTI DI VIDEOSORVEGLIANZA.

Il Presente verbale viene letto, approvato e sottoscritto:

Il Sindaco

Antonio Landro



Il Segretario Comunale

Dott. ssa Adriana Avventura

REFERTO DI PUBBLICAZIONE

Certifico lo sottoscritto Segretario Comunale, che copia del presente verbale viene pubblicata all'Albo Pretorio, ove rimarrà esposta per 15 giorni consecutivi.

Il Segretario Comunale

Dott. ssa Adriana Avventura

ESECUTIVITA'

Il sottoscritto, visti gli atti d'ufficio, attesta che la presente deliberazione:

è stata pubblicata all'albo pretorio informatico comunale per 15 giorni consecutivi (art. 124, D.Lgs. n. 267/2000);

è stata dichiarata immediatamente eseguibile ai sensi dell'art. 134 del D.Lgs. n. 267/2000;

è divenuta esecutiva il, decorsi dieci giorni dalla pubblicazione (art. 134, comma 3, D.Lgs. n. 267/2000).



Il Segretario Comunale

Dott. ssa Adriana Avventura