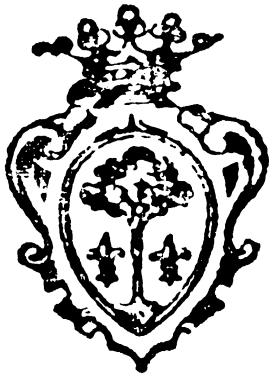
COMUNE DI FARNESE

Provincia di VITERBO



REGOLAMENTO COMUNALE IN MATERIA DI VIDEOSORVEGLIANZA SUL TERRITORIO COMUNALE

Approvato con Deliberazione del Consiglio Comunale
n. 14 del 21.05.2020

INDICE

CAPO I
PRINCIPI GENERALI

Art. 1
Premessa

1. Il presente Regolamento disciplina le modalità di raccolta, trattamento e conservazione dei dati' personali mediante sistemi di videosorveglianza gestiti, nell'ambito del proprio territorio, dal Comune di Farnese;
2. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, cioè che si realizza a distanza mediante dispositivi per le riprese video collegati a un centro di controllo e coordinamento.
3. Le immagini, qualora rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi la videosorveglianza incide sul diritto delle persone alla propria riservatezza.
4. 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 Farnese, 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
5. Ai fini delle definizioni di cui al presente Regolamento si deve fare riferimento all'art. 4 del Regolamento UE 2016/679 (e al conseguente D.lgs 101/2018) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e all'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. 2
Norme di riferimento e principi generali

Il presente regolamento disciplina il trattamento di dati personali, realizzato mediante impianto di videosorveglianza cittadina ed altre tipologie di videosorveglianza (foto-trappole, body - cam, dash cam e riprese aeree), attivati o attivabili nel territorio del Comune di Farnese.
Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto dal:

- Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008), incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione;
- Legge n. 38/2009 recante "misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori";
- Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);
- Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito GDPR) relativo "alla Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera di circolazione di tali dati e che abroga la direttiva 95/46/CE";
- D.P.R. n. 15 del 15/01/2018 recante "Regolamento a norma dell'articolo 57, del D. Lgs. 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";
- D. Lgs. 18/05/2018 n. 51 "Attuazione della 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;
• D. Lgs. 10/08/2018 n.101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE".

La Videosorveglianza in ambito Comunale si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5 GDPR e dell.art.3 del D. Lgs. n. 51/2018 e, in particolare:
Pr***incipio di liceità*** — II trattamento di dati personali da parte di soggetti pubblici è lecito allorquando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ossequio al disposto di cui all'art. 6. Paragrafo 1, lett. e). GDPR. La videosorveglianza comunale pertanto è consentita senza necessità di consenso da parte degli interessati.
Principio di necessità — In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5. Paragrafo 1, lett. c), GDPR, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati 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. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.
Principio di proporzionalità — La raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla 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 quando altre misure siano 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 quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento.
Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere.
Principio di finalità — Ai sensi dell'art. 5, Paragrafo 1, lett. b), GDPR, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la **sicurezza urbana**, che il DM Interno 05/08/2008 definisce come il **"bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale.**

Art. 3
Definizioni

Ai fini del presente regolamento si intende:
a) Per "**banca dati**", il complesso di dati personali, formatosi presso la sala di controllo e trattato esclusivamente mediante riprese video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;

b) Per “**trattamento**”, tutte le operazioni o complesso di operazioni, svolte con l’ausilio dei mezzi elettronici, informatici 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, l’eventuale diffusione, la cancellazione e la distribuzione di dati;
c) Per “**dato personale**”, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, rilevati con trattamenti di immagini effettuati attraverso l’impianto di videosorveglianza;
d) Per “**titolare**”, il Comune di Farnese e, quale suo organo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali, il Sindaco pro tempore;
e) Per “**responsabile**”, la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento dei dati personali;
f) Per “**incaricati**”, le persone fisiche autorizzate a compiere operazioni distrattamente o dal titolare o dal responsabile;
g) Per “**interessato**”, la persona fisica, la persona giuridica, l’Ente o associazione cui si riferiscono i dati personali;
h) Per “**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;
i) Per “**diffusione**”, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
l) Per “**dato anonimo**”, il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
m) Per “**blocco**”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

Art. 4
Finalità istituzionali dei sistemi di videosorveglianza

Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza attengono allo svolgimento delle funzioni istituzionali proprie dell'amministrazione comunale in conformità a quanto previsto dal:

- Legge 7 marzo 1986, n. 65, sull'ordinamento della Polizia Municipale;
- D.P.R. 24 luglio 1977, n.616;
- D.Lgs. 31 marzo 1998, n. 112;
- D.Lgs. 18 agosto 2000, n. 267 TUEL;
- Legge 24 luglio 2008, n. 125 recante misure urgenti in materia di sicurezza pubblica;
- Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana;
- Legge 23 aprile 2009 n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale;
- Circolari del Ministero dell'Interno n.558/A/421.2/70/456 in data 8 febbraio 2005, n 558/A421.2/70/195860 in data 6 agosto 2010 e n. 558/SICPAR1/421.2/70/224632 in data 02.03.2012.
- D. Lgs. n.51/2018.

Nella richiamata cornice normativa e all'interno del nuovo sistema di lotta alla criminalità che attribuisce ai Comuni un ruolo strategico nel perseguire finalità di tutela della sicurezza pubblica, l'impianto di videosorveglianza del Comune di Farnese è precipuamente rivolto a garantire la sicurezza urbana che, l'art. 1 del D. M. dell'Interno del 5 agosto del 2008, testualmente definisce come il "bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."
La disponibilità tempestiva di immagini presso il Comune costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale sul territorio comunale, in stretto raccordo con le Forze dell'Ordine. L'archivio dei dati registrati costituisce, infatti, per il tempo di conservazione stabilito per legge,

un patrimonio informativo per finalità di Polizia Giudiziaria, con eventuale informativa nei confronti dell'Autorità Giudiziaria competente, a procedere in caso di rilevata commissione di reati.
In particolare, il sistema di videosorveglianza attivato dall'Amministrazione, è finalizzato a:
a) incrementare la sicurezza urbana e la sicurezza pubblica non ché la percezione delle stesse rilevando situazioni di pericolo e consentendo l'intervento degli operatori;
b) prevenire, accertare e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" già richiamato; le informazioni potranno essere condivise con altre forze di Polizia competenti a procedere nei casi di commissione di reati;
c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e gli edifici pubblici e a prevenire eventuali atti di vandalismo o danneggiamento;
d) controllare le aree considerate a maggiore rischio per la sicurezza, l'incolumità e l'ordine pubblico;
e) al monitoraggio del traffico;
f) attivare uno strumento operativo di protezione civile sul territorio comunale;
g) ad acquisire elementi probatori in fattispecie di violazioni amministrative o penali;
h) per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
i) monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
j) verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.
Gli impianti di videosorveglianza non potranno essere utilizzati, in base all'art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970) per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati. Gli impianti di videosorveglianza non potranno altresì essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.
L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.
La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi.
La possibilità di avere in tempo reale dati e immagini, costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell'ambito delle proprie competenze istituzionali; attraverso tali strumenti si perseguono finalità di tutela della popolazione e del patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.
L'uso dei dati personali nell'ambito definito dal presente Regolamento non necessita del consenso degli interessati in quanto viene effettuato per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri e allo svolgimento di funzioni istituzionali di cui è investito il Comune.

Art. 5
Caratteristiche tecniche dell'impianto

Presso la sede municipale, nell'ufficio della Polizia Locale, è posizionato il sistema ed il monitor per la registrazione, gestione e visione in diretta delle immagini riprese dalle telecamere.
I dati sono accessibili dal Titolare e dal Responsabile. Ai quali sono fornite le chiavi di accesso.
Le telecamere a seconda degli obiettivi da perseguire; sono collegate direttamente alla sala operativa sita in municipio presso gli uffici della Polizia Locale, nonché alla sala operativa della Polizia Stradale competente

per territorio, tramite cavo di rete, fibra ottica o ponti radio, attraverso un'infrastruttura studiata per mappare il più possibile l'abitato.
Il sistema di videosorveglianza potrà constare in futuro anche di altre tipologie di apparecchiature come le foto trappole o le dash-cam per l'utilizzo in pattuglia con l'auto di servizio o con sistemi di ripresa aerea – droni.
La scelta e la posizione delle telecamere è stata fatta, a seguito di accordi tra l'Amministrazione e le Forze di Polizia, prioritariamente in base all'esigenza di monitorare il traffico da e per il centro abitato, ma anche, le piazzole ecologiche, i parchi e le principali strutture pubbliche.
Il collegamento all'impianto di videosorveglianza può essere esteso alle Forze di Polizia che ne facciano richiesta all'Amministrazione Comunale, nei limiti e con l'osservanza delle norme contenute nel presente Regolamento ovvero disciplinate con successivo atto in conformità al quadro normativo di riferimento.
In relazione ai principi di pertinenza e di non eccedenza già richiamati all'art. 2 del presente Regolamento, il sistema informativo ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessita.

Art. 6
Utilizzo di particolari sistemi mobili.

A- Body Cam e Dash Cam

1 Gli operatori di Polizia Locale possono utilizzare, per i servizi a maggior rischio operativo, delle Body Cam (telecamere a bordo uomo) e delle Dash Cam (telecamere a bordo veicoli di servizio) in conformità delle indicazioni dettate dal Garante della Privacy con nota 26 luglio 2016, prot. n. 49612, con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi il cui trattamento dei dati è ricondotto nell'ambito dell'art. 53 del Codice Privacy e 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".
Il responsabile del Servizio 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 devono essere attivate, dei soggetti eventualmente 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.

1) Le videocamere e le schede di memoria di cui sono dotati i sistemi di cui al comma precedente 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.
2) La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato.
3) Il sistema di registrazione dovrà essere attivato solo in caso dì effettiva necessità, ossia nel caso di insorgenza delle situazioni descritte al comma 1.
4) Spetta all'Ufficiale di Polizia Giudiziaria o in mancanza all'Agente di P.G. in servizio, l'attivazione dei dispositivi, in relazione all'evolversi degli scenari di sicurezza e ordine pubblico che facciano presupporre criticità.
5) Il trattamento dei dati personali effettuati con simili sistemi di ripresa devono rispettare i principi di cui all'art.11 del Codice 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 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.

B - Telecamere modulari (foto trappole).

Su tutto il territorio comunale in futuro potranno essere posizionate telecamere modulari (foto trappole) con generazione di allarmi da remoto per il monitoraggio attivo.

Gli appartai di videosorveglianza modulare mobile vengono posizionati secondo necessità, esclusivamente nei luoghi teatro di illeciti penali o amministrativi, questi ultimi non altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza di cui all'art 53 del D.lgs. 196/2003 o necessità di indagine previste dal D.lgs 51/2018 che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, quale informativa agli utenti frequentatori di dette aree

Art. 7
Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona video sorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti,manifestazioni sportive).
A tal fine l'Ente utilizza lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, **riportato in fac-simile nell'allegato n. 1** al già richiamato Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010 e di seguito riportato, con indicazione, nel lato inferiore del cartello, il riferimento normativo - Art. 13 del Regolamento europeo sulla protezione dei dati personali (RGDP 2016/679)-:

Polizia Locale – Comune di Farnese - Area video sorvegliata, Immagini custodite presso gli uffici della Polizia Locale.

L'informativa completa sul trattamento dei dati raccolti con il sistema di videosorveglianza può essere letta nel sito internet istituzionale del Comune di Farnese, nella sezione – Privacy - .
L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere.
La segnaletica deve essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa 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.
In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi.
L'Ente, nella persona del Responsabile del trattamento dei dati, si obbliga ad **informare la comunità cittadina** dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per

qualsiasi causa del trattamento medesimo, **con un anticipo di giorni dieci,** mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.

Art. 8
Valutazione di Impatto sulla protezione dei dati

In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c). GDPR, qualora il trattamento di dati realizzato mediante il sistema di videosorveglianza comunale dia luogo ad una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, l'Ente procederà ad una valutazione di impatto sulla protezione dei dati personali. Parimenti si procederà nei casi in cui, il trattamento di dati realizzato mediante il sistema di videosorveglianza presenti un rischio comunque elevato per i diritti e le libertà delle persone fisiche.

(fac – simile ALLEGATO 2)

Art. 9
Titolare e funzionario designato del Trattamento dei dati

Il Titolare del trattamento dei dati è il Comune di Farnese, al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare. Il funzionario, individuato dal Titolare, designato al coordinamento delle attività e al controllo del trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza.
Il funzionario designato al coordinamento delle attività e al controllo del trattamento, è tenuto a conformare la propria azione al pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente Regolamento. Il funzionario designato al coordinamento delle attività e al controllo procede al trattamento dei dati attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.
Le competenze proprie del funzionario designato al coordinamento delle attività e al controllo del trattamento sono analiticamente disciplinate nell'atto amministrativo di nomina, con il quale il Titolare provvede alla sua individuazione. In particolare, il funzionario designato al coordinamento delle attività e al controllo del trattamento dovrà:
- individuare e nominare, con propri atti, gli incaricati del trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, GDPR; detti incaricati saranno opportunamente istruiti e formati da parte del funzionario designato del trattamento con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;
- provvedere a rendere l'informativa "minima" agli interessati secondo quanto definito al precedente art. 6;
- verificare e controllare che il trattamento dei dati effettuato mediante sistema di videosorveglianza sia realizzato nel rispetto dei principi di cui all'art. 5 del GDPR e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente;
- garantire altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;
- assicurare che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
-adottare, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del GDPR;
- garantire l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico;

- assicurare l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;
- garantire che il Responsabile della Protezione dei Dati, designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti.

Il funzionario designato è, in oltre, responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, perciò dovrà:
- assicurare che gli incaricati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le attività strettamente necessarie al perseguimento delle finalità istituzionali;
- garantire la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale individuato quale incaricato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;
- vigilare sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Art. 10
Incaricati del Trattamento

Il funzionario designato al coordinamento delle attività e al controllo del trattamento dei dati procede ad individuare con proprio atto le persone fisiche incaricate del trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni. L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato.
In ogni caso, prima dell'utilizzo degli impianti, gli incaricati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.
Gli incaricati procedono al trattamento attenendosi alle istruzioni impartite dal funzionario designato al coordinamento delle attività e al controllo il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari. In particolare, gli incaricati devono:
• predisporre un registro relativo agli accessi come indicato nell'ALLEGATO 5;
• per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
• conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
• mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
• custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
• evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile del trattamento dei dati;
• mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;
• conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
• fornire al funzionario designato del trattamento dei dati ed al Responsabile della Protezione dei dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

Tra i soggetti designati quali incaricati verranno individuati, con l'atto di nomina, le persone cui è affidata la custodia e la conservazione delle chiavi di accesso alla sala operativa. Gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del funzionario designato al coordinamento delle attività e al controllo.
L'utilizzo degli apparecchi di ripresa da parte degli incaricati al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato.

Art. 11
Modalità di Raccolta e di Trattamento dei Dati

L'installazione delle telecamere avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili) in conformità all'elenco dei siti di ripresa predisposto dall'Amministrazione Comunale. L'attività di videosorveglianza deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.
Le telecamere di cui al precedente comma 1, consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario. Il Titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa saranno inviati presso l'unità " Sala operativa" di ricezione, registrazione e visione ubicata presso gli uffici della Polizia Locale. In questa sede, sarà realizzata un'area con accesso riservato dove le immagini saranno visualizzate su monitor e registrate su supporto magnetico. I dati personali oggetto di trattamento sono:
- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per le finalità di cui all'art. 4 del presente Regolamento e resi utilizzabili in altre attività di trattamento a condizione che si tratti di attività non incompatibili con tali scopi;
- raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.

La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata al massimo, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle richiamate disposizioni normative, il **termine massimo di durata della conservazione** dei dati è limitato ai **sette giorni successivi alla rilevazione delle informazioni** e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve specifiche esigenze di ulteriore conservazione.
In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria, il Titolare potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai sette giorni previa richiesta al Garante per la protezione dei dati personali che, a seguito di verifica preliminare, potrà rilasciare parere favorevole.
Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
In caso di cessazione del trattamento, i dati personali sono distrutti.

Art. 12
Sicurezza dei dati

I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del precedente art.11. I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure

tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, assicurano:
a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Ai sensi dell'art.32, Paragrafo 2, GDPR, nel valutare l'adeguato livello di sicurezza, l'Amministrazione terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ente.
A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:
a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori, devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini.
Tenendo conto dello stato dell'arte ed in base alle caratteristiche dei sistemi utilizzati, i soggetti designati quali incaricati del trattamento dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le attività di competenza;
b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime attività di cancellazione o di duplicazione;
c) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 10, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;
d) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette attività potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;
e) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;
f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie Wi—Fl.Wi Max, Gprs).
Il Titolare del trattamento vigila sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvede altresì ad istruire e formare gli incaricati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati.

Art. 13
Accesso ai dati

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 necessita per il conseguimento delle finalità di cui all'art. 4 del presente Regolamento.
L'accesso alle immagini è consentito esclusivamente:
a) al Titolare ed agli incaricati del trattamento;
b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);

c) alla società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo ovvero, in casi del tutto eccezionali, all'amministratore informatico del sistema comunale (preventivamente individuato quale incaricato del trattamento dei dati);
d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso, fac simile allegato 3, alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta al successivo art. 13. L'accesso da parte dell'interessato, sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, da parte del Responsabile del Servizio di Polizia Locale o dai suoi incaricati, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;
e) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente, l'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

Art.14
Diritti dell'interessato

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., GDPR, su presentazione di apposita istanza, ha diritto:
a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
b) ad essere informato 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;
c) di richiedere la cancellazione, qualora sussista uno dei motivi di cui all'art. 17 GDPR, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, GDPR.
L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP .
Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:
- il luogo, la data e la fascia oraria della possibile ripresa;
- l'abbigliamento indossato al momento della possibile ripresa;
- gli eventuali accessori in uso al momento della possibile ripresa;
- l'eventuale presenza di accompagnatori al momento della possibile ripresa;
- l'eventuale attività svolta al momento della possibile ripresa;
- eventuali ulteriori elementi utili all'identificazione dell'interessato.

Il Responsabile della Protezione dei dati dell'Ente ovvero il Responsabile del Servizio di Polizia Locale, 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.
Qualora, ai sensi dell'art. 15. paragrafo 3, GDPR, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15. paragrafo 4. GDPR.

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
Nell'esercizio dei diritti di cui al comma 1, l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi; l'interessato può altresì farsi assistere da persona di fiducia. Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Art. 15
Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss. GDPR ed alle previsioni Decreto Legislativo 101/2018 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE", in attuazione della delega al Governo di cui all'art. 13 L. 163/2017.

Art. 16
Provvedimenti attuativi

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

Art. 17
Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali

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. GDPR. Il Titolare del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
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, GDPR.
Nel caso in cui l'interessato sia certo di un uso scorretto e/o dannoso delle immagini relative a se stesso ha diritto di procedere con la richiesta di accesso agli atti per reclamo (ALLEGATO 4) e seguire l'iter previsto dai precedenti commi.

Art. 18
Pubblicità del Regolamento

Copia del presente Regolamento sarà pubblicata all'albo pretorio e potrà essere reperita nel sito internet istituzionale del Comune di Farnese.

Art. 19
Modifiche regolamentari

1. I contenuti del presente regolamento dovranno essere aggiornati nei casi di aggiornamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari generali del Consiglio comunale dovranno essere immediatamente recepiti.
2. Il presente regolamento è trasmesso al Garante per la protezione dei dati personali a Roma e al Comitato per l'Ordine Pubblico della Provincia, sia a seguito della sua approvazione, sia a seguito dell'approvazione di suoi successivi ed eventuali aggiornamenti.

Art. 20
Entrata in vigore

Il presente Regolamento entrerà in vigore con l'esecutività della deliberazione di approvazione, secondo le leggi vigenti.
Dalla data di entrata in vigore del presente Regolamento sono abrogati tutti gli atti in precedenza emessi sulla materia e tutte le norme con esso incompatibili.
Eventuali modifiche disposte con atti di legislazione aventi carattere sovraordinato nelle materie oggetto del presente Regolamento, si devono intendere recepite in modo automatico.

ALLEGATO 1

CONTENUTI INFORMATIVI SEMPLIFICATI AI SENSI DEL D. LGS. 196/2003 DA APPORRE SU TUTTO IL TERRITORIO COMUNALE IN BASE AL POSIZIONAMENTO DELLE TELECAMERE

ALLEGATO 2

FAC – SIMILE DI PROSPETTO VALUTAZIONE RISCHI CHE INCOMBONO SUI DATI

RISCHI: *Si - No*

DESCRIZIONE DELL'IMPATTO SULLA SICUREZZA gravità: *alta - media – bassa*

Sottrazione di credenziali di autenticazione		*Media*
Carenza di consapevolezza, disattenzione o incuria		*Media*
Comportamenti sleali o fraudolenti		*Alta*
Comportamento degli operatori – Errore materiale		*Bassa*
Azione di virus informatici o di programmi suscettibili di recare danno		*Bassa*
Spamming o tecniche di sabotaggio		*Media*
Malfunzionamento, indisponibilità o degrado degli strumenti		*Bassa*
Accessi esterni non autorizzati		*Bassa*
Eventi relativi agli strumenti – Intercettazioni di informazioni in rete		*Media*
Accessi non autorizzati a locali/reparti ad accesso ristretto		*Media*
Accessi non autorizzati ad armadi contenenti apparati sul territorio comunale		*Media*
Sottrazione di strumenti contenenti dati presso la centrale operativa		*Bassa*
Sottrazione di strumenti contenenti dati presso gli armadi periferici		*bassa*
Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc), nonché dolosi, accidentali o dovuti ad incuria		*Bassa*
Guasto ai sistemi complementari (climatizzazione, impianto elettrico, ecc.)		*Bassa*
Eventi relativi al contesto – Errori umani nella gestione della sicurezza fisica		

MISURE MINIME DA ADOTTARE DA PARTE DEI SOGGETTI CHE TRATTANO IDATI
Non scrivere la password
Cambiare periodicamente le password
Formazione degli operatori all'avviamento del sistema
Formazione periodica degli operatori
Comportamenti sleali o fraudolenti
Dotazione di un manuale d'uso a tutti gli operatori
Divieto di installare programmi di qualsiasi genere sui PC di visualizzazione
Server di registrazione chiuso a chiave
Il sistema non deve essere collegato ad alcuna rete pubblica di telecomunicazioni
Accesso alle centrali operative presidiate e in sicurezza
Accessi non autorizzati ad armadi contenenti apparati sul territorio comunale
Dotazione di dispositivi UPS per guasto al sistema

(Contenuti minimi e indicativi che potranno essere integrati – modificati dalla Giunta Comunale quale Organo Esecutivo di Vertice)

ALLEGATO 3

FAC – SIMILE - RICHIESTA DI ACCESSO A VIDEOREGISTRAZIONI -

Il sottoscritto ……, identificato tramite ……, ai sensi della vigente normativa in materia di privacy richiede di esercitare il diritto di accesso alle immagini video che potrebbero aver registrato dati personali a sé stesso afferenti.

Per permettere di individuare tali immagini nell'archivio video, fornisce le seguenti informazioni:

1.luogo o luoghi di possibile ripresa……
……
……
……
2.data di possibile ripresa……
……
3.fascia oraria di possibile ripresa (approssimazione di 30 minuti)……..
……
4.abbigliamento al momento della possibile ripresa……
……
……
5.accessori (borse, ombrelli, carrozzine, animali al guinzaglio, altri oggetti)
……
……
……
……
6.presenza di accompagnatori (indicare numero, sesso, sommaria descrizione)
……
……
……
……
7. attività svolta durante la ripresa…….
……
……
……
……
……
Recapito (o contatto telefonico) per eventuali ulteriori approfondimenti
……
……

In fede.

(luogo e data)……..

(firma leggibile) ……..

PARTE DA CONSEGNARE AL RICHIEDENTE

In data …… alle ore …….. il/la Sig./Sig.ra……..ha avanzato richiesta di accesso a videoregistrazioni, ai sensi della vigente normativa in materia di privacy.

……

(firma del ricevente la richiesta)

ALLEGATO 4

FAC – SIMILE DOMANDA DI ACCESSO AI DATI REGISTRATI PER RECLAMO

Al Responsabile trattamento dei dati
……..

Il/La sottoscritto/a……..……..……,che aveva presentato in data ……..….. presso ……. Una richiesta di accesso alle immagini video che potrebbero aver registrato miei dati personali presenta reclamo per i seguenti motivi:
……
……
……
……
……
……
…….

Recapito (o contatto telefonico) per eventuali ulteriori approfondimenti
……..……..……...
……..……..……
…..……
In fede.
(luogo e data)……..

(firma)
……

PARTE DA CONSEGNARE AL RICHIEDENTE
In data …… alle ore …….. il/la Sig./Sig.ra……..……..ha avanzato richiesta di accesso avideoregistrazioni, ai sensi della vigente normativa in materia di privacy.

……
(firma del ricevente la richiesta)

ALLEGATO 5

FOGLIO TIPO PER REGISTRO DEGLI ACCESSI ALLA VISIONE DELLE IMMAGINI VIDEOREGISTRATE

NOME E COGNOME	DOCUMENTO IDENTITA'	ESTREMI AUTORIZZAZIONE	ORA ENTRATA	ORA USCITA

DICHIARO

- di mantenere l'assoluta riservatezza su qualunque dato personale di cui possa essere venuto a conoscenza durante la permanenza nel locale, ai sensi della vigente normativa sulla privacy.
- di mantenere l'assoluta riservatezza su qualunque dato personale di cui possa essere venuto a conoscenza durante la permanenza nel locale, ai sensi della vigente normativa sulla privacy.
- di mantenere l'assoluta riservatezza su qualunque dato personale di cui possa essere venuto a conoscenza durante la permanenza nel locale, ai sensi della vigente normativa sulla privacy.
- di mantenere l'assoluta riservatezza su qualunque dato personale di cui possa essere venuto a conoscenza durante la permanenza nel locale, ai sensi della vigente normativa sulla privacy.
- di mantenere l'assoluta riservatezza su qualunque dato personale di cui possa essere venuto a conoscenza durante la permanenza nel locale, ai sensi della vigente normativa sulla privacy.

FIRMA LEGGIBILE	DATA