Città di Potenza

REGOLAMENTO COMUNALE PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA NEL TERRITORIO COMUNALE

Approvato dal C.C. con deliberazione n. 8 del 2 marzo 2023

Articolo 1 - Oggetto

1. Il presente Regolamento disciplina il trattamento dei dati personali, effettuato mediante gli impianti di videosorveglianza installati nel territorio urbano ed extraurbano del Comune di Potenza, gestiti dal Corpo di Polizia Locale, ed affinché lo stesso 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.

2. Privati e/o soggetti terzi, singoli o associati, possono, previa approvazione di specifiche linee guida da parte della Giunta Comunale, partecipare all'estensione, sperimentazione e all'implementazione del sistema di videosorveglianza cittadino mediante l'acquisto diretto e la conseguente cessione al Comune della strumentazione utile (telecamere, illuminatori I/R, ponti radio, reti in fibra ottica e licenze software ed altri eventuali strumenti) ad integrare l'impianto esistente.

3. In particolare il presente regolamento:

a) individua gli impianti che compongono il sistema di videosorveglianza comunale;
b) definisce le caratteristiche e le modalità di utilizzo del sistema di videosorveglianza;
c) disciplina gli adempimenti, le garanzie e le tutele per il legittimo, pertinente e non eccedente trattamento dei dati personali acquisiti mediante l'utilizzo del sistema.

4. L'impianto di videosorveglianza del Comune di Potenza è finalizzato all'espletamento delle funzioni istituzionali e strumentali di Polizia Locale, del monitoraggio veicolare per la gestione del traffico, nonché di controllo del territorio per fini di sicurezza, ordine, decoro, quiete pubblica e perseguimento di condotte non conformi alle leggi ed ai regolamenti.

5 Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali.

6. Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nel singolo caso possono essere realizzati medianti dati anonimi ed opportune modalità che permettano di identificare l'interessato soltanto in caso di necessità.

7. E' istituito il nucleo intersettoriale di videosorveglianza comunale costituito dal dirigente/comandante, o suo delegato, del Corpo di Polizia Locale, dal dirigente, o suo delegato, dell'U.D. Manutenzione del Patrimonio e Viabilità, dell'U.D. Bilancio e Partecipate-Ufficio Gestione del Patrimonio, dell'U.D. Urbanistica e Gestione del Territorio ed il D.P.O. (*Data Protection Officer)* comunale con il compito di predisporre e aggiornare l'elenco dei siti di ripresa, definire ogni ulteriore e specifica disposizione ritenuta utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento, proporre l'adeguamento delle tecnologie e la gestione dei protocolli di sicurezza, verificare l'impatto privacy dei sistemi di videosorveglianza.

8. Per tutto quanto non dettagliatamente disciplinato nel presente Regolamento, si rinvia a quanto disposto dal:

a) Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";
b) "Regolamento Europeo in materia di protezione dei dati personali", UE 679/2016, (General Data Protection Regulation) del 27 aprile 2016, come rettificato con provvedimento pubblicato sulla Gazzetta Ufficiale dell'Unione europea, n. 127, del 23 maggio 2018, 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;
c) Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
d) Linee guida 07/2020 sui concetti di titolare e responsabile nel General Data Protection Regulation, adottate il 07 luglio 2021, dal Comitato Europeo per la produzione dei dati;
e) Regolamento sulla protezione dei dati personali, approvato con delibera di Consiglio Comunale di Potenza, n. 28 del 30/04/2020;
f) Legge 163/2017 ed in particolare l'art. 13;
g) Legge 167/2017 ed in particolare l'art. 28;
h) Decreto-legge 20 febbraio 2017, n. 14 convertito con la legge 18 aprile 2017, n. 48;
i) D.Lgs. 30 giugno 2003, n, 196, recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;
j) D.Lgs. 18 agosto 2000, n. 267 e successive modificazioni, ed in particolare l'art. 54;
k) D.L. 23 febbraio 2009, n. 11, convertito con modificazioni dalla L. 23 aprile 2009, n. 38, recante: "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori", ed in particolare dall'art.6;
l) Provvedimenti e codici di deontologia promossi dal Garante per la protezione dei dati personali, tra cui, in particolare: Le linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29 gennaio 2020; Provvedimento a carattere generale 29/11/2000: Videosorveglianza – Il decalogo delle regole per non violare la Privacy. Provvedimento a carattere generale 29/04/2004: Videosorveglianza – Provvedimento generale. Provvedimento in materia di Videosorveglianza – 8 aprile 2010;
m) Circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/A/471 e ss.mm.ii.;
n) Direttive del Ministero degli Interni avente oggetto "Sistemi di videosorveglianza in ambito comunale";
o) Circolare n. 2/2017 del 18 aprile 2017 (Agenzia per l'Italia Digitale), in sostituzione della circolare 1/2017 del 17 marzo 2017 recante: "Misure minime di sicurezza ICT per le pubbliche amministrazioni" (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015" (GU 103 del 05/05/2017);

p) Circolare della Direzione Generale per l'Attività Ispettiva, del Ministero del Lavoro e delle Politiche sociali, prot. n. 37/0007162 del 16/04/2012 come modificata dalla circolare n. 5/2018 del 19/02/2018;
q) D.Lgs. 101 del 10/08/2018 "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 (regolamento generale sulla protezione dei dati);
r) D.Lgs. 51 del 18 maggio 2018 Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti 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;
s) Direttiva 680/2016 del Parlamento Europeo e del Consiglio d'Europa 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 della libera circolazione di tali dati, che introduce la regolamentazione della protezione delle persone fisiche con riferimento al trattamento dei dati da parte delle autorità ai fini di prevenzione, investigazione e repressione dei reati.

Articolo 2 - Definizioni

1. A norma del *General Data Protection Regulation,* viene stabilito che la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configurano un trattamento di dati personali.

2. Ai fini del presente regolamento e richiamate le definizioni del *General Data Protection Regulation* si intende:
a) per "**Codice**": il Codice in materia di protezione dei dati personali di cui al D.Lgs. 10 agosto 2018 e successive modificazioni e integrazioni;
b) per "**GDPR**": il Regolamento generale per la protezione dei dati personali n. 2016/679, normativa europea in materia di protezione dei dati;
c) per "**impianto di videosorveglianza**": qualunque impianto di ripresa, fissa o mobile, composto da una o più telecamere, in grado di riprendere e registrare immagini ed eventualmente suoni, utilizzato per le finalità di cui al presente regolamento;
d) per "**banca di dati**": il complesso di dati personali, formatosi presso la centrale operativa della Polizia Locale, raccolti esclusivamente mediante riprese videoregistrate, che in relazione ai luoghi di installazione delle videocamere interessano prevalentemente i soggetti ed i mezzi di trasporto che transitano nell'area interessata;
e) per "**dato personale**": qualunque informazione relativa a persona fisica, persona giuridica, Ente o associazione, identificati o identificabili anche direttamente, e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza. I dati di connessione (indirizzo IP, login ed altro), i dati di localizzazione (ubicazione, GPS,

GSM, ed altro). La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali;

f) per "**trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

g) per "**limitazione di trattamento**": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento;

h) per "**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;

i) per "**archivio**": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

j) per "**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;

k) per "**dati genetici**": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

l) per "**dati biometrici**": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

m) per "**dati relativi alla salute**": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

n) per "**titolare del trattamento**": il Comune di Potenza, nella persona del Sindaco pro-tempore, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;

o) per "**responsabile del trattamento**": la persona fisica, preposta dal titolare del trattamento - con atto scritto - al trattamento dei dati personali;

p) per "**autorizzati**": le persone fisiche autorizzate - con atto scritto - a compiere operazioni di trattamento dal titolare o dal responsabile;

q) per "**interessato**": la persona fisica, la persona giuridica, l'Ente o associazione cui si riferiscono i dati personali;

r) 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;

s) per “**diffusione**”: il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

t) 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;

u) per “**blocco**”: la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;

v) per “**terzo**”: la persona fisica, la persona giuridica, l’ente o associazione che non sia interessato al trattamento, 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;

w) per “**destinatario**”: la persona fisica o giuridica, l’autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali;

x) per “**rappresentante**”: la persona fisica o giuridica stabilita nell’Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell’articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento, rappresentante del Titolare;

y) per “**consenso dell’interessato**”: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell’interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

z) per “**geolocalizzazione**”: l’identificazione della posizione geografica nel mondo reale di un dato oggetto, come ad esempio una radio digitale, un telefono cellulare o un computer/tablet connesso o meno ad Internet, secondo diverse tecniche.

3. Il presente regolamento non si applica ai trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Articolo 3 - Principi generali

1. Le prescrizioni del Regolamento (artt. 5-6) si fondano sui principi di liceità, necessità, proporzionalità e finalità del trattamento:

a) Principio di liceità: il trattamento di dati personali dalla parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali; esso infatti è necessario per l’esecuzione di un compito di interesse pubblico connesso all’esercizio di pubblici poteri di cui i Comuni e il Comando di Polizia Locale sono investiti;

b) Principio di necessità: il sistema di videosorveglianza è configurato per l’utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l’interessato solo in caso di necessità;

c) Principio di proporzionalità: nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli o per le quali non ricorra una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano 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;
d) Principio di finalità: gli scopi perseguiti devono essere determinati, espliciti e legittimi. Sono pertanto escluse finalità di prevenzione o accertamento dei reati, che competono per specialità ad altri organi. E' consentita la videosorveglianza come misura complementare volta a migliorare la sicurezza delle aree pubbliche (es. parcheggi, piazze, parchi urbani, aree verdi, ecc.) all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, come pure nei pressi di siti utilizzati come discariche abusive o che hanno comunque lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.

2. L'attività di videosorveglianza e di geolocalizzazione è esercitata osservando le seguenti indicazioni:

a) sono fornite alle persone che possono essere riprese indicazioni chiare, circa la presenza di impianti di videosorveglianza;
b) è scrupolosamente rispettato l'art 4 dello Statuto dei Lavoratori, come modificato dal Jobs Act (cfr.: sentenza Cassazione penale n. 22148/2017) in merito al controllo a distanza dei lavoratori;
c) sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti.

Articolo 4 - Finalità e sistemi di sorveglianza

1. L'uso del sistema di videosorveglianza è strumento per l'attuazione di un sistema integrato di politiche per la sicurezza urbana, per la tutela dell'ordine, del decoro e della quiete pubblica. La possibilità di disporre in tempo reale di dati ed immagini costituisce un ulteriore strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell'ambito delle proprie competenze istituzionali; attraverso tali strumenti si persegue l'intento di tutelare l'utenza ed il patrimonio comunale, garantendo, quindi, un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone periferiche della città, nei pressi degli edifici pubblici ed in prossimità delle scuole, nel centro storico, negli ambienti e nelle strade ad intenso traffico veicolare.

2. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di un impianto di videosorveglianza nel territorio urbano, gestito dal Comune di Potenza, Comando di Polizia Locale, e collegato alla centrale operativa della stessa Polizia Locale

nonché a quella delle forze dell'ordine, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

3. Garantisce altresì i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento. Il sistema informativo e 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 necessità**.**

4. Possono essere installati sistemi integrati, sistemi intelligenti e sistemi per rilevare le violazioni al Codice della Strada (con le modalità previste dal Provvedimento in materia di Videosorveglianza 8 aprile 2010 e ss.mm.ii.):

a) i sistemi integrati collegano telecamere tra soggetti diversi che consentono la sorveglianza da parte di società specializzate, mediante collegamento ad un unico centro. È necessaria la verifica preliminare del Garante;
b) i sistemi intelligenti sono dotati di software che permettono l'associazione di immagini a dati biometrici, in grado, ad esempio, di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli. È necessaria la verifica preliminare del Garante;
c) la presenza di sistemi di rilevazione delle violazioni al Codice della Strada deve essere segnalata da appositi cartelli. Le telecamere devono riprendere solo la targa del veicolo e gli altri elementi necessari per la predisposizione del verbale di accertamento delle violazioni, ad esempio il tipo del veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta. Le fotografie e i video non possono essere inviati al domicilio dell'intestatario del veicolo, il quale potrà richiedere di visionare la documentazione. Al momento dell'accesso, se ripresi, dovranno opportunamente essere oscurati o resi comunque non riconoscibili i passeggeri a bordo del veicolo.

5. In relazione ai principi di pertinenza e di non eccedenza, il sistema informativo e 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 necessità.

6. Il Comune promuove, per quanto di propria competenza, il coinvolgimento dei privati per la realizzazione di singoli impianti di videosorveglianza, orientati comunque su aree o strade pubbliche o a uso pubblico, nel rispetto dei principi di cui al presente Regolamento, previa valutazione di idoneità dei siti e dei dispositivi. Tali impianti, una volta realizzati, possono essere utilizzati e gestiti esclusivamente dal Comune di Potenza. Il Comune accetta la cessione d'uso dei dispositivi e degli accessori solo se ha preventivamente valutato con esito positivo l'idoneità del sito e la compatibilità dei dispositivi con l'impianto comunale. In seguito a tale valutazione favorevole da parte del Comune, i privati interessati si impegnano formalmente ad assumere ogni onere e ogni spesa per:

a) acquistare i dispositivi e ogni necessario accessorio, con connessione al sistema centrale ovvero con memorizzazione locale delle immagini, in conformità alle caratteristiche tecniche dell'impianto comunale;

b) mettere i predetti dispositivi a esclusiva disposizione del Comune a titolo gratuito, senza che i privati stessi possano vantare alcun titolo o diritto di ingerenza sulle immagini, sulle riprese video, sulla gestione e sul trattamento dei dati, sulla tecnologia connessa e sulla gestione dei dispositivi, che restano di esclusiva competenza del Comune di Potenza.

7. Il Comune di Potenza assume su di sé esclusivamente le spese per la manutenzione ordinaria.

Articolo 5 - Diretta visione delle immagini

1. Il presente Regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto di videosorveglianza attivato nel territorio urbano del Comune di Potenza e collegato alla centrale operativa della Polizia Locale, nonché i sistemi ad esso collegati presso altre Centrali operative delle Forze dell'ordine.

2. La diretta visualizzazione delle immagini rilevate con i sistemi di videosorveglianza e/o geolocalizzazione nelle sale o centrali operative è limitata ad obiettivi particolarmente sensibili e strategici per la sicurezza urbana o in presenza del requisito di pubblico interesse (necessità, pertinenza, non eccedenza dei dati o dei trattamenti) e previa concertazione decentrata o autorizzazione della DTL, se richiesta per la localizzazione dei lavoratori.

3. Il responsabile si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto.

Articolo 6 - Trattamento dei dati personali per le finalità istituzionali degli impianti di videosorveglianza e geolocalizzazione

1. Il trattamento dei dati personali è effettuato a seguito dell'attivazione di un impianto di videosorveglianza o di un sistema di geolocalizzazione.

2. Le finalità istituzionali dell'impianto di videosorveglianza, sono conformi alle funzioni istituzionali del Comune di Potenza così come indicate dal D. Lgs. 18 agosto 2000 n. 267, dal D.P.R. 24 luglio 1977 n. 616, dalla L. 689 del 24 novembre 1981, dalla Legge 7 marzo 1986 n. 65 sull'ordinamento della Polizia Locale, dalla Legge della Regione Basilicata n. 41/2009 e dal vigente Codice della Strada, nonché dallo Statuto Comunale e dai Regolamenti Comunali vigenti, ed hanno lo scopo di:

a) prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del D.L. n. 4/2017 convertito in L. 48/2017;
b) prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado e abbandono di rifiuti, e svolgere i controlli volti ad accertare e sanzionare le violazioni contenute nel Regolamento di Polizia Urbana, nei

regolamenti locali in genere e nelle ordinanze sindacali quando non risulti possibile, o si rilevi non efficace, il ricorso a strumenti e sistemi di controllo alternativi;

c) assicurare la disponibilità tempestiva di immagini presso la Centrale Operativa della Polizia Locale, costituendo uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale e delle Forze di polizia, di tutela dell'incolumità pubblica, perseguendo anche finalità di *security* e *safety;*
d) monitorare il traffico cittadino in tempo reale dalla sala operativa del Comando Polizia Locale, con conseguente più razionale e pronto impiego delle risorse umane laddove se ne presenti la necessità;
e) tutelare l'ordine, il decoro e la quiete pubblica;
f) ricostruire, ove possibile, la dinamica degli incidenti stradali;
g) rilevare, con dati anonimi, dei dati dei flussi di traffico veicolare da utilizzarsi per la predisposizione dei piani del traffico;
h) prevenire eventuali atti di vandalismo o danneggiamento agli immobili in particolare quelli afferenti al patrimonio comunale;
i) rilevare le infrazioni a norma di legge o regolamenti di competenza specifica della Polizia Locale, con particolare riferimento alla tutela dell'ambiente e del territorio, quando non risulti possibile, o si rilevi non efficace, il ricorso a strumenti e sistemi di controllo alternativi;
j) rilevare le infrazioni al Codice della Strada ai sensi e per gli effetti dell'art. 201 CDS, art. 2, della legge L. 689/81;
k) garantire la protezione e l'incolumità degli individui, il benessere animale e/o la corretta osservanza di ordinanze e/o regolamenti comunali per consentire l'accertamento dei relativi illeciti con particolare riguardo ai profili attinenti alla sicurezza urbana, l'ordine e la sicurezza pubblica, la prevenzione, l'accertamento o repressione dei reati, la razionalizzazione e il miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge, ai soggetti pubblici ed ai Comuni, in particolare;
l) tutelare e proteggere la proprietà pubblica;
m) acquisire prove della commissione di illeciti penali ed amministrativi;
n) promozione turistica o pubblicitaria anche con l'utilizzo di webcam o camera on line. In questo caso non devono essere rese visibili le persone riprese. In caso di riprese televisive il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese televisive e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti e gli eventuali mezzi di trasporto che transiteranno nell'area interessata;
o) per controllare discariche di sostanze pericolose ed "eco-piazzole" per monitorare le modalità del loro uso, la tipologia dei rifiuti scaricati e l'orario di deposito;
p) per tutelare coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un elevato grado di sicurezza nelle zone monitorate.

3. Per la **geolocalizzazione** di veicoli ed operatori, le finalità perseguite sono quelle di gestione ottimale delle risorse sul territorio da parte della centrale operativa, sicurezza sul lavoro, tutela del patrimonio e rilievi statistici anonimi.

4. Per la geolocalizzazione il *Data Protection Officer* supporterà il responsabile del trattamento del dato nella redazione della valutazione di impatto. Il datore di lavoro è sempre tenuto ad assicurare ai dipendenti il diritto di opporsi al trattamento.

Articolo 7 – Responsabile del sistema di videosorveglianza

1. Il titolare del trattamento dei dati personali derivanti dall'uso del sistema di videosorveglianza è il Comune di Potenza, nella persona del Sindaco; quest'ultimo, ex art. 29 Reg. Ue 2016/679 e art. 2-*quaterdecies* Codice Privacy, designa per iscritto il soggetto Responsabile del sistema di videosorveglianza di cui al presente regolamento, di norma il Comandante della Polizia Locale.

2. Il soggetto designato ai sensi del comma precedente assume le funzioni, i compiti, i doveri e le responsabilità che il Regolamento UE 2016/679 assegna al titolare del trattamento, limitatamente alle fattispecie di trattamento dei dati personali coinvolte dall'utilizzo del sistema di videosorveglianza e di geolocalizzazione.

3. Il soggetto designato ai sensi del comma 1, può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità, in tal caso individuando le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta e per definirne i compiti affidati.

4. Il Responsabile della gestione del sistema di videosorveglianza assicura il rispetto di quanto prescritto dalle normative vigenti e dalle disposizioni del presente Regolamento, in conformità alle istruzioni ricevute in sede di designazione e, in particolare:

a) adotta le misure e dispone gli interventi necessari per la sicurezza del trattamento dei dati e la correttezza dell'accesso ai dati;
b) cura il rispetto degli obblighi di trasparenza, con particolare riferimento all'informativa da fornire agli interessati ed alla gestione dei procedimenti per il riconoscimento dei diritti riconosciuti agli interessati dal Regolamento UE 2016/679;
c) cura la gestione delle modalità di ripresa e di registrazione delle immagini;
d) custodisce le chiavi di accesso ai locali delle centrali di controllo e le chiavi dei locali e degli armadi nei quali sono custoditi i supporti contenenti le registrazioni;
e) cura la distruzione/cancellazione dei dati nel caso venga meno lo scopo del trattamento o l'obbligo di conservazione;
f) effettua, prima di procedere al trattamento, quando questo può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, una valutazione dell'impatto del trattamento sulla protezione dei dati personali. Prima di procedere al trattamento, consulta l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
g) coopera, su richiesta, con il Responsabile della protezione dei dati personali e con l'Autorità di controllo nell'esecuzione dei rispettivi compiti. Si assicura che il responsabile della protezione dei dati personali sia tempestivamente ed

adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;

h) identifica contitolari, responsabili e sub responsabili coinvolti nella gestione ed utilizzo del sistema di videosorveglianza, e sottoscrive gli accordi interni ed i contratti/appendici contrattuali per il trattamento dei dati, avendo cura di tenere costantemente aggiornati i documenti relativi ai contitolari ed ai responsabili;
i) nomina gli incaricati del trattamento in numero sufficiente a garantire la gestione del servizio di videosorveglianza nell'ambito del personale di Polizia Locale;
j) in caso di violazione dei dati personali collabora con il titolare del trattamento ed il responsabile della protezione dei dati personali nel processo di notifica della violazione all'Autorità di controllo competente senza ingiustificato ritardo e, comunque, entro 24 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;
k) in caso di violazione dei dati personali, comunica la violazione all'Interessato senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

5. Il Segretario comunale/generale è responsabile dell'attivazione della contrattazione decentrata o dell'istanza di autorizzazione alla Direzione Territoriale del Lavoro, se richiesta per l'attività di geolocalizzazione.

Articolo 8 - Autorizzati

1. Compete al responsabile del sistema di videosorveglianza del Comune di Potenza designare per iscritto gli autorizzati del trattamento dei dati, dell'utilizzazione degli impianti, della visione delle registrazioni e dell'esportazione delle stesse, con profili di accesso diversi.

2. Gli autorizzati devono conformare la propria azione al rispetto di quanto prescritto dalle normative vigenti e dalle disposizioni del presente Regolamento e dal Responsabile del sistema di videosorveglianza.

Articolo 9 – Profili di autorizzazione

1. La gestione degli impianti di videosorveglianza e di geolocalizzazione è riservata, di norma, alla Polizia Locale di Potenza.

2. Le nomine ad autorizzato devono essere personali; esse devono essere sempre conservate agli atti del Comando e tenute in copia presso la Centrale Operativa della Polizia Locale. I compiti affidati agli autorizzati devono essere analiticamente specificati nell'atto di designazione.

3. Ad ogni nomina di autorizzato deve corrispondere un profilo personale identificato da nome e cognome e password che deve essere cambiata al primo accesso e, successivamente, ogni 6 mesi.

4. Gli autorizzati devono conformare la propria azione al rispetto di quanto prescritto dalle normative e dalle disposizioni del Regolamento. I livelli di autorizzazione sono i seguenti:

VISIONE LIVE – REGISTRAZIONI – ESPORTAZIONE – AMMINISTRATORE – MANUTENZIONE.

5. Gli autorizzati dovranno essere istruiti al corretto uso dei sistemi, sulla conoscenza della normativa di riferimento e sul presente Regolamento.

6. Nell'ambito degli autorizzati, verranno designati, con l'atto di nomina, i soggetti cui è affidata la custodia e conservazione delle password e delle chiavi di accesso alla Sala Operativa ed agli armadi per la conservazione dei supporti contenenti le immagini.

Articolo 10 - Persone autorizzate ad accedere alla sala di controllo

1. L'accesso alla sala di controllo è consentito solamente al personale in servizio alla Polizia Locale, autorizzato per iscritto dal Comandante responsabile del sistema o suo incaricato (art.7), e agli autorizzati addetti ai servizi.

2. Eventuali accessi di persone diverse da quelle innanzi indicate devono essere autorizzati, per iscritto, dal Comandante della Polizia Locale.

3. Possono essere autorizzati all'accesso solo autorizzati di servizi rientranti nei compiti istituzionali dell'ente 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 o alla sperimentazione di nuove tecnologie, e il personale delle Forze dell'ordine.

4. Il Responsabile della gestione e del trattamento impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.

5. Gli autorizzati dei servizi di cui al presente regolamento vigilano sul puntuale rispetto delle istruzioni e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Articolo 11 - Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento sono:

a) trattati su uno dei presupposti di liceità che il codice prevede espressamente negli artt. 18 – 22 "Regole ulteriori per i soggetti pubblici", e secondo correttezza;
b) raccolti e registrati per le finalità di cui al precedente art. 4 e resi utilizzabili in altre operazioni non incompatibili con tali scopi, esatti e, se necessario, aggiornati;
c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
d) l'attività di videosorveglianza è effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione;

e) Le immagini videoregistrate, per finalità di sicurezza urbana, sono conservate dal sistema presso la Centrale Operativa del Comando di Polizia Locale per un periodo massimo di sette giorni, trascorsi i quali le immagini verranno sovrapposte (*expiring*). Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione mediante sovra registrazione con modalità tali da rendere non utilizzabili i dati cancellati;
f) le immagini esportate per altre forze di Polizia a fini di indagini di Polizia Giudiziaria saranno consegnate con apposito verbale. Prima di consegnare le immagini su supporto asportabile, si avrà cura di attivare le protezioni tecnicamente disponibili a garanzia che il supporto asportato possa essere utilizzato in condizioni di "sola lettura". Copia identica di dette immagini, definita "di fede" (con le protezioni appena indicate) sarà inserita in una busta sigillata e contrassegnata dal numero identificativo del verbale di consegna per essere custodita all'interno della sala di videosorveglianza. Le immagini richieste dovranno essere ritirate entro 7 giorni dalla data della richiesta; oltre tale termine le stesse verranno cancellate;
g) nel caso in cui si voglia procedere ad un allungamento dei tempi di conservazione per un periodo superiore alla settimana, per motivi diversi da quelli di indagine di Polizia Giudiziaria, si dovrà richiedere espressa autorizzazione al Garante. Tale allungamento dei termini dovrà essere ipotizzato dal Titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità;
h) trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, di cui agli artt. 3 e 18, con modalità volta a salvaguardare l'anonimato ed, in ogni caso, successivamente alla fase della raccolta, atteso che le immagini registrate possono contenere dati di carattere personale;
i) è possibile il libero trattamento di immagini anonimizzate.

2. Il trattamento dei dati viene effettuato con strumenti elettronici, nel rispetto delle misure minime indicate dal Regolamento Europeo in materia di Privacy.

3. La mancata osservanza degli obblighi di cui al presente Regolamento comporta l'applicazione delle sanzioni disciplinari ed amministrative previste dalla normativa vigente, e ove previsto dalla medesima, l'avvio degli eventuali procedimenti penali.

4. Tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposito **"*REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO E DEGLI ACCESSI*"** (cartaceo od informatico), conservato nei locali del Comando di Polizia Locale, nel quale sono riportati:

- la data e l'ora d'accesso;
- l'identificazione del terzo autorizzato;
- i dati per i quali si è svolto l'accesso;

- gli estremi e la motivazione dell'autorizzazione all'accesso;
- le eventuali osservazioni dell'incaricato;
- la sottoscrizione del medesimo.

5. Non possono essere rilasciate copie delle immagini registrate concernenti altri soggetti diversi dall'interessato, salvi i casi particolarmente meritevoli di tutela.

6. La diffusione di immagini personali è consentita quando la persona interessata ha espresso il proprio consenso o è necessaria per la salvaguardia della vita o dell'incolumità fisica o è giustificata da necessità di giustizia o di polizia; essa è comunque effettuata con modalità tali da non recare pregiudizio alla dignità della persona.

7. In caso di cessazione, per qualsiasi causa, dell'attività di videosorveglianza, il Comune effettuerà la notificazione al Garante ai sensi della vigente normativa. A seguito di ciò i dati raccolti dovranno essere distrutti o conservati per fini esclusivamente istituzionali

Articolo 12 - Obblighi degli operatori

1. L'utilizzo del brandeggio o delle telecamere mobili da parte degli operatori e degli autorizzati al trattamento dovrà essere conforme ai limiti indicati nel documento di cui al comma 3 del precedente articolo. L'utilizzo delle telecamere, sia fisse che mobili, è consentito solo per il controllo di quanto si svolge nei luoghi pubblici, mentre non è ammesso nelle proprietà private.

2. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite di tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità per il conseguimento delle finalità di cui al presente regolamento e a seguito di regolare autorizzazione di volta in volta richiesta al Responsabile del trattamento dei dati personali designato.

3. La mancata osservanza degli obblighi previsti nel presente articolo, comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.

Articolo 13 - Accertamenti di illeciti e indagini di Autorità Giudiziarie o di Polizia

1. Ove dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, l'incaricato dovrà immediatamente informare il Responsabile della videosorveglianza, che dovrà dare pronta comunicazione agli organi competenti.

2. In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa di cui al precedente art. 9, l'autorizzato procederà alla registrazione delle stesse su supporti informatici.

3. L'accesso ai dati è consentito, oltre che ai soggetti di cui ai precedenti articoli del presente Regolamento, esclusivamente all'Autorità Giudiziaria, agli Organi di polizia giudiziaria e ad eventuali Ausiliari di polizia giudiziaria.

4. Nel caso in cui gli organi di Polizia, nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate che sono contenute nelle riprese effettuate, possono farne richiesta scritta e motivata indirizzata al Responsabile della gestione e del trattamento dei dati.

Articolo 14 - Informazioni rese al momento della raccolta – Informativa

1. Il Comune di Potenza si obbliga ad affiggere un'adeguata informativa come indicato all'art. 13 e 14 del Regolamento Europeo in materia di privacy, nelle strade e nelle piazze nei pressi delle quali sono posizionate le telecamere.

2. Il Comune di Potenza, nella persona del Titolare, si obbliga a comunicare alla cittadinanza l'avvio del trattamento dei dati personali, con l'attivazione degli impianti di videosorveglianza, l'eventuale incremento dimensionale dell'impianto e l'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, mediante l'affissione di appositi manifesti informativi e/o notizia sul sito istituzionale e/o altri mezzi di diffusione locale.

3. Gli interessati dovranno sempre essere informati che stanno per accedere ad una zona videosorvegliata. A tal fine si ricorrerà all'utilizzo dello stesso modello semplificato di informazione "minima", indicante il titolare del trattamento e la finalità perseguita. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, sono installate più informative. La cartellonistica è posizionata in maniera visibile sulle vie d'accesso della Città e nei punti di maggiore frequentazione. I cartelli possono essere posizionati in luoghi ripresi o nelle immediate vicinanze di essi, e non necessariamente nelle immediate vicinanze della telecamera.

4. L'uso delle immagini per le finalità dichiarate nel presente regolamento non necessita di consenso da parte delle persone riprese in quanto viene effettuato per lo svolgimento di funzioni istituzionali. La presenza e la disciplina dell'impianto di videosorveglianza viene resa pubblica mediante l'affissione del presente Regolamento all'Albo Pretorio del Comune, la pubblicazione dello stesso sul sito internet comunale ed il deposito di una copia presso la sede del Corpo di Polizia Locale.

5. Il supporto con l'informativa:
   a) dovrà essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
   b) dovrà 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 anche di notte;
   c) potrà inglobare un simbolo o una stilizzazione di esplicita ed immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o registrate.

Articolo 15 -Diritti dell'interessato

1. L'interessato del trattamento dai dati personali, dietro presentazione di apposita istanza ed il versamento di un contributo per le spese vive, ha diritto:

a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;
b) di essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
c) di ottenere, a cura del Responsabile, senza ritardo e comunque non oltre 15 giorni dalla data di ricezione della richiesta:
   - la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati;
   - la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento. La richiesta non può essere inoltrata dallo stesso soggetto se non sono trascorsi almeno novanta giorni da una precedente istanza, fatta salva l'esistenza di giustificati motivi;
   - la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   - di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Per ciascuna delle richieste di cui al presente Regolamento, 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 del costo del personale, definiti con atto formale dalla Giunta Comunale secondo le modalità previste dalla normativa vigente.

2. I diritti di cui al presente articolo, riferiti ai dati personali concernenti persone decedute, possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

3. 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.

4. Le istanze di cui al presente articolo possono essere trasmesse mediante lettera raccomandata o posta elettronica certificata al titolare e al responsabile, i quali dovranno provvedere in merito entro e non oltre quindici giorni.

5. 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. Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento (art. 9 del Regolamento Europeo).

6. La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal

Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

7. In riferimento alle immagini registrate, non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo. Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge.

Articolo 16 - Caratteristiche tecniche minime dell'impianto e dislocazione

1. Le caratteristiche tecniche minime dell'impianto di videosorveglianza del Comune di Potenza rispondono alle caratteristiche minime previste dalla Circolare del Ministero dell'Interno n. 558/ SICPART/421.2/70/224632 del 02/03/2012.

Articolo 17 - Sicurezza dei dati e Data Protection Officer

1. Conformemente al principio di *accountability,* introdotto dall'art. 5 punto 2 General Data Protection Regulation, il Titolare del trattamento dei dati designa una persona fisica con la funzione di DPO (*Data Protection Officer*) in modo da garantire in ogni fase del trattamento la piena conformità al trattamento e raccogliere prove documentali per dimostrarla, nonché ad analizzare i rischi connessi ai trattamenti da loro posti in essere (c.d. risk-based approach).

2. Tale figura, pur considerando i propri obblighi di segretezza e riservatezza, che tuttavia non gli impediscono di contattare e richiedere consigli all'autorità Garante, dovrà:

a) informare e fornire consulenza al titolare e al responsabile del trattamento nonché ai dipendenti degli obblighi derivanti dal regolamento;
b) sorvegliare l'osservanza del General Data Protection Regulation, nonché delle altre disposizioni europee o di diritto interno in materia di protezione di dati;
c) sorvegliare sulle attribuzioni della responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo;
d) fornire pareri e sorvegliare alla redazione della Data Protection impact assessment (c.d. Dpia);
e) fungere da punto di contatto e collaborare con l'Autorità Garante per la protezione dei dati personali;
f) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate (c.d. Data Breach Notification Management).

3. Le misure minime di sicurezza dovranno rispettare i seguenti principi:

a) In presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati autorizzati o eventualmente responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;

b) Laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve 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 operazioni di cancellazione o duplicazione;
c) In merito al periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
d) Nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare le specifiche cautele. In particolare, i soggetti preposti alle predette operazioni potranno accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini: in questo caso gli accessi al sistema dovranno essere autorizzati dal titolare e/o dal responsabile del trattamento, tracciati e registrati su apposito registro cartaceo degli accessi presente presso i locali della Centrale Operativa videosorveglianza del Comando di P.L. o su registro elettronico integrato al sistema;

4. Qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale.

5. La trasmissione, tramite una rete pubblica di comunicazione, di immagini riprese da apparati di videosorveglianza deve essere 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 connessione wireless (tecnologie Wi-Fi, wi-max, Gprs).

6. Le caratteristiche tecniche dell'impianto di videosorveglianza relativamente alla sicurezza dello stesso rispondono a quanto indicato nel documento tecnico annesso alla direttiva n. 558 del 2 marzo 2012 del Ministero dell'Interno e ss.mm.ii.

Articolo 18 - Uso delle telecamere

1. Il sistema di videosorveglianza prevede di massima una ripresa statica dei luoghi e non rileva automaticamente percorsi o caratteristiche fisionomiche od altri dati che consentano l'individuazione di persone definite. Sono fatti salvi attività di sperimentazione dirette al riconoscimento comportamentale illecito, in modo da permettere l'archiviazione automatica dei comportamenti per l'analisi degli stessi da parte di personale abilitato (cfr art. 20).

2. È previsto l'uso del brandeggio della telecamera, quando possibile, da parte di un operatore solo nei seguenti casi:
a) per il controllo e la registrazione di atti illeciti perpetrati all'interno del campo iniziale di registrazione della telecamera e che rischierebbero di sfuggire al controllo per lo spostamento dei soggetti interessati;
b) in caso di comunicazione, anche verbale e telefonica, di situazioni di illecito o di pericolo segnalate al responsabile dell'impianto, che necessitino di essere verificate nell'immediatezza;
c) nel supporto logistico ad operazioni istituzionali condotte con personale sul luogo. È altresì previsto l'uso di dispositivi di videosorveglianza mobile (tipo "Sentinel" o foto trappole)

collocabili nelle zone individuate di volta in volta, secondo necessità, dal Comando di Polizia Locale per l'esercizio delle attività di controllo e istituzionali, garantendo i principi di cui al presente regolamento, anche con l'ausilio di personale tecnico specializzato, nominato ad hoc.

3. Le inquadrature devono essere tali da cogliere un'immagine panoramica delle persone e dei luoghi, evitando riprese inutilmente particolareggiate tali da essere eccessivamente intrusive nella riservatezza delle persone, garantendo comunque la possibilità di identificazione per esigenze inerenti alle finalità dichiarate.

4. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 3 comma 2 e a seguito di regolare autorizzazione di volta in volta richiesta al Responsabile del trattamento dei dati personali designato.

Articolo 19 - Sistemi integrati di videosorveglianza

1. Nell'ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

a) gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche. In tale ipotesi, i singoli titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;
b) collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo. Tale soggetto terzo, designato dal responsabile del trattamento da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare;
c) sia nelle predette ipotesi sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia. L'attivazione del predetto collegamento deve essere reso noto agli interessati. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati.

2. Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle indicate dal Regolamento Europeo:

a) adozione di sistemi idonei alla registrazione degli accessi logici degli autorizzati 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 responsabili da parte del titolare, comunque non inferiore a sei mesi;

b) separazione logica delle immagini registrate dai diversi titolari.

3. Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a chiedere una verifica preliminare al Garante.

Articolo 20 - Sistemi di videosorveglianza posti in essere da enti pubblici e da enti territoriali

1. Anche gli enti territoriali e i soggetti pubblici operanti sul territorio possono effettuare attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle diverse attività istituzionali.

2. Nei casi di cui al comma 1 è necessario che:

a) l'utilizzo condiviso, in forma totale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;

b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.

3. Il titolare del trattamento è tenuto a richiedere una verifica preliminare al Garante al di fuori delle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra menzionati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali il garante la richiede.

Articolo 21 - Istituti scolastici

1. Il sistema di videosorveglianza attivo presso istituti scolastici, installato previa comunicazione al responsabile dell'Istituto, dovrà garantire il diritto dello studente alla riservatezza di cui all'art. 2 DPR n. 249/1998, prevenendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, ai processi di maturazione ed al loro diritto all'educazione. In tale quadro, potrà risultare ammissibile l'utilizzo di tali sistemi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti.

2. È vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola.

3. Laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo della visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio.

Articolo 22- Utilizzo di particolari sistemi mobili Body cam, Dash cam e droni

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 dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria".
2. 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. 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 a maggior rischio operativo.

3. Spetta all'ufficiale di Polizia Giudiziaria o all'agente più anziano impartire l'ordine di attivazione dei dispositivi, in relazione all'evolversi degli scenari di sicurezza e ordine pubblico che facciano presupporre criticità. Lo stesso ne disporrà la disattivazione. Al termine del servizio gli operatori interessati, previa compilazione di un foglio di consegna, depositeranno tutta la documentazione video al Comando.

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 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.

5. Per l'utilizzo di tale strumento deve essere adottato un disciplinare rispettoso delle indicazioni fornite dal Garante della Privacy (provvedimento 362 del 22 maggio 2018). Inoltre, il Comune dovrà agire anche nel rispetto dell'art 4 dello Statuto dei Lavoratori per rispettare il divieto di controllo a distanza del lavoratore, fatti salvi i fatti illeciti commessi dal personale nell'orario di esercizio e che possano comportare l'applicazione di sanzioni disciplinari. In tale prospettiva, deve essere siglato apposito accordo con le organizzazioni sindacali o, in alternativa, deve essere acquisita l'autorizzazione da parte dell'Ufficio provinciale del lavoro.

6. Il "DRONE" è un complesso costituito da uno strumento volante ed un pilota che lo controlla. Lo strumento volante tecnicamente prende il nome di "AEROMOBILE A PILOTAGGIO REMOTO" – APR, mentre il complesso costituto dal velivolo e dal pilota costituisce il "SISTEMA DI AEROMOBILE A PILOTAGGIO REMOTO" – SAPR. Per l'utilizzo dei Droni dovrà farsi riferimento al nuovo Regolamento di esecuzione (UE) 2020/746, recante modifiche al precedente Regolamento di esecuzione (UE) 2019/947 relativo ai Sistemi Aeromobili a Pilotaggio Remoto (SAPR), comunemente noti come droni.

Articolo 23- Videosorveglianza ambientale e deposito rifiuti

1. Il Garante Privacy con il Provvedimento in materia di videosorveglianza dell'8 aprile 2010, pubblicato sulla Gazzetta Ufficiale del 29 aprile 2010, stabilisce che "in applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate 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 alternativi. 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, l. 24 novembre 1981, n. 689)".

2. Il Comune di Potenza, al fine di prevenire e reprimere gli illeciti ambientali derivanti dall'inosservanza di specifiche leggi in materia (Testo Unico Ambientale – D.Lgs. 152/2006 e successive modifiche ed integrazioni) e gli illeciti amministrativi derivanti dalle violazioni alle disposizioni emanate dal Comune relativamente alle modalità di conferimento dei rifiuti, si avvale dell'utilizzo di telecamere fisse integrate al sistema di Videosorveglianza Comunale e di un sistema di telecamere mobili. Le telecamere mobili sono da considerarsi parte del sistema di videosorveglianza cittadino.

3. L'attività di prevenzione e accertamento mediante videosorveglianza degli illeciti derivanti dall'abbandono e dal deposito dei rifiuti sul territorio comunale in maniera difforme da quanto previsto dalle vigenti disposizioni normative, verrà posta in essere in siti considerati critici e di particolare interesse dove le classiche misure di controllo del territorio, a cura degli organi preposti, non sono sufficienti ad ottenere positivi risultati.

4. Le postazioni e le località sul territorio comunale dove verrà utilizzata la videosorveglianza al fine di prevenzione, accertamento e repressione degli illeciti di cui sopra sono individuate dagli organi istituzionali del Comune e dai responsabili dei servizi degli uffici preposti a tale attività di controllo e potranno variare nel tempo in base alle necessità di perseguimento dei fini istituzionali dell'ente.

5. L'elenco delle postazioni individuate secondo i principi di cui sopra, nelle quali può essere posto in essere il controllo con videosorveglianza mediante l'uso di apparecchi di ripresa mobili, è allegato al presente regolamento costituendone parte integrante e viene aggiornato e reso pubblico mediante le prescritte modalità istituzionali ogni qual volta sarà soggetto a modifiche e

cambiamenti: l'elenco delle postazioni è sempre vincolato da approvazione da parte della Giunta Comunale mediante atto formale.

6. Nelle aree sottoposte a videosorveglianza per fini di prevenzione, accertamento e repressione degli illeciti derivanti dall'utilizzo abusivo dell'area impiegata come discarica di materiale e di sostanze pericolose, nonché di rispetto della normativa concernente lo smaltimento dei rifiuti, sono posizionati appositi cartelli di informativa minima, collocati prima del raggio d'azione delle telecamere o in prossimità delle stesse, riportanti la dicitura "la registrazione è effettuata dalla Polizia Locale di Potenza per fini di prevenzione, accertamento e repressione degli illeciti concernenti lo smaltimento dei rifiuti".

7. Le immagini registrate sono conservate per un periodo non superiore ai sette giorni successivi alla rilevazione, fatte salve le esigenze di ulteriore conservazione quali la necessità di custodire o consegnare una copia specificatamente richiesta all'autorità giudiziaria o alla polizia giudiziaria in relazione ad un'attività investigativa in corso, ovvero per adempiere alla procedura sanzionatoria amministrativa ex art. 13 Legge 689/81, riconducibile alle finalità del trattamento.

8. I dati personali oggetto del trattamento di cui al presente articolo sono custoditi ai sensi e per gli effetti della normativa vigente e possono essere visionati, estratti e trattati solo da personale autorizzato.

Articolo 24- Accertamenti di illeciti e indagini di polizia giudiziaria

1. Ove dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, il responsabile del sistema di videosorveglianza di cui all'articolo 3 provvederà a darne immediata comunicazione agli organi competenti.

2. In tali casi è consentita la estrazione delle registrazioni dal sistema e memorizzazione delle stesse su supporti informatici, il cui contenuto deve essere protetto da password, per la trasmissione agli organi di polizia e l'autorità giudiziaria. Ferma restando l'attività di estrazione, alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di polizia e l'autorità giudiziaria.

3. Gli apparati potranno essere utilizzati anche in relazione ad indagini di autorità giudiziaria o di organi di polizia.

4. Nel caso in cui gli organi di polizia, nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate che sono contenute nelle riprese effettuate, possono farne richiesta scritta e motivata, indirizzata al responsabile del sistema di videosorveglianza di cui all'articolo 3.

5. Nelle ipotesi previste dal presente articolo, è consentito procedere agli ingrandimenti della ripresa delle immagini strettamente necessarie e non eccedenti lo specifico scopo perseguito, su richiesta degli organi di polizia e dell'autorità giudiziaria.

Articolo 25 - Comunicazione e diffusione

1. La comunicazione e la diffusione di dati personali da parte del Comune di Potenza a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di Legge o Regolamento. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria, ed esclusivamente per lo svolgimento delle funzioni istituzionali o se i dati sono anonimizzati.

2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza di dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal Titolare o dal Responsabile e che operano sotto la loro diversa autorità.

3. È in ogni caso fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del D. Lgs. 30/6/2003, n. 196, come modificato dal D.Lgs. 101/2018, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Articolo 26 - Tutela

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dal Regolamento Europeo in materia di Privacy.

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 responsabile del trattamento dei dati personali, così come individuato dal precedente art. 11.

Articolo 27 - Cessazione del trattamento dei dati personali

1. In caso di cessazione dell'attività per qualsiasi causa, i dati personali sono:
   a) distrutti;
   b) ceduti ad altro titolare purché destinati ad un trattamento compatibile con gli scopi per i quali sono stati raccolti.
   c) conservati per fini esclusivamente istituzionali.

2. La cessione dei dati per scopi diversi da quelli previsti dal presente articolo o da altre disposizioni vigenti determina la loro inutilizzabilità, fatta salva l'applicazione delle sanzioni previste in materia.

Articolo 28 - Modifiche regolamentari e rinvio dinamico

1. I contenuti del presente Regolamento dovranno essere aggiornati nei casi di adeguamento 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. Le disposizioni del presente regolamento si intendono comunque modificate per effetto di sopravvenute norme vincolanti statali e regionali. In tali casi, in attesa della formale modificazione del presente regolamento, si applica la normativa sovraordinata.

Articolo 29 - Pubblicità del Regolamento

1.Copia del presente Regolamento, a norma dell'art. 22 della Legge 07/08/1990, n. 241, e successive modificazioni ed integrazioni, sarà tenuta a disposizione del pubblico perché ne possa prendere visione in qualsiasi momento.

2. Copia dello stesso sarà pubblicata sul sito internet del Comune e sarà altresì trasmessa alle Forze di polizia collegate al Sistema.

Articolo 30 -Abrogazioni

1. Con l'entrata in vigore del presente Regolamento sono abrogate tutte le disposizioni, ordinanze e norme regolamentari del Comune di Potenza in contrasto con le disposizioni in esso contenute. Rimangono, invece, in vigore tutte quelle disposizioni compatibili che possono trovare applicazione in casi o fattispecie non disciplinati dal presente Regolamento.

Articolo 31-Entrata in vigore

1. Il presente Regolamento entrerà in vigore dopo i previsti termini di pubblicazione all'Albo Pretorio del Comune di Potenza.