



CITTÀ DI PISTICCI

(Provincia di Matera)

VERBALE DI DELIBERAZIONE DEL CONSIGLIO COMUNALE

VERBALE N. 7 DEL 27-03-2023

OGGETTO: Regolamento Comunale in materia di videosorveglianza.

ASSESSORE PROPONENTE :

L'anno duemilaventitre il giorno ventisette del mese di marzo alle ore 17:00 con prosecuzione, nella Residenza Municipale, legalmente convocato dal Presidente del Consiglio si è riunito il Consiglio Comunale, in seduta Ordinaria in Prima convocazione.

Alla trattazione del presente punto risultano presenti o assenti i componenti del Consiglio Comunale come appresso indicati:

Presenti N. **16**

Assenti N. **1**

Favorevoli **13**

Contrari **0**

Astenuti **3**

Albano Domenico Alessandro	Presente	SINDACO	Zaffarese Antonio	Presente	CONSIGLIERE
Giannone Domenicangelo Donato	Presente	CONSIGLIERE	Rago Renato	Presente	CONSIGLIERE
Camardella Maria Teresa, Barbara	Presente	CONSIGLIERE	Di Trani Vito Anio	Presente	CONSIGLIERE
D'onofrio Angela	Presente	CONSIGLIERE	Calandriello Carmine	Presente	CONSIGLIERE
Muliero Roberto Tommaso	Presente	CONSIGLIERE	Grieco Pasquale Domenico	Presente	CONSIGLIERE
Badursi Andrea	Presente	CONSIGLIERE	Miolla Giuseppe	Presente	CONSIGLIERE
Iannuzziello Eligio	Presente	CONSIGLIERE	Verri Viviana	Presente	CONSIGLIERE
Losenno Marco	Presente	CONSIGLIERE	Tuccino Pasquale Salvatore	Assente	CONSIGLIERE
Sodo Pasquale	Presente	CONSIGLIERE			

Accertata la presenza di n. 16 consiglieri componenti del Consiglio Comunale sui 17 in carica, il Presidente del Consiglio, procede alla trattazione dell'argomento in atti. Prende parte ai lavori il **SEGRETARIO GENERALE** Dott.ssa URICCHIO Grazia, con funzioni di Segretario verbalizzante.

IL TITOLARE DI P.O.

Parere in ordine alla sola regolarità tecnica ai sensi dell'art.49, nonché art. 147/bis del D. Lgs. 18.08.2000 N° 267 e ss.mm.ii.
Favorevole

Pisticci, lì 07-03-2023

IL TITOLARE DI P.O.
*Ten. Volpe Domenica**

**Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa.*

IL CONSIGLIO COMUNALE

PREMESSO che il Comune di Pisticci ha previsto di attivare nel proprio territorio un impianto di videosorveglianza mediante uso di telecamere e di altre tipologie di dispositivi idonei di videosorveglianza (fototrappole, body cam, dash cam), nell'ambito dello svolgimento delle funzioni istituzionali proprie dell'amministrazione comunale, in conformità a quanto previsto dalle seguenti norme:

- 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 08/022005, n. 558/A421.2/70/195860 in data 06/082010 e n. 558/SICPART/421.2 /70/224632 in data 02.03.2012;
 - D. Lgs. n.51/2018.
- che le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza, nella richiamata cornice normativa e all'interno del nuovo sistema di lotta alla criminalità, attengono alla tutela della sicurezza pubblica e alla garanzia della sicurezza urbana che l'art. 1 del Decreto del Ministero 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.”*;
 - che le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali; la videosorveglianza dà luogo, pertanto, a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa pur essendo la videosorveglianza comunale consentita senza necessità di consenso da parte degli interessati;

CONSIDERATO:

- che il Comune di Pisticci non è ancora dotato di un Regolamento che garantisca il trattamento dei dati personali acquisiti mediante sistemi di videosorveglianza, di varia tipologia, gestiti ed impiegati nel territorio comunale nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche con particolare riferimento alla riservatezza e all'identità personale;
- che 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;
- che la tempestiva disponibilità di immagini presso il Comune costituisce 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, inoltre, costituisce, 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.
- che il sistema di videosorveglianza attivato dall'Amministrazione è, inoltre, finalizzato:
 - a tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e gli edifici pubblici e a prevenire eventuali atti di vandalismo o danneggiamento;
 - attivare uno strumento operativo di protezione civile sul territorio comunale;
 - controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche e accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
 - monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
 - verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.

Discusso ed approfondito l'argomento in Commissione Consiliare di Pisticci in data 20/10/2022;

VISTO:

- il Codice in materia di protezione dei dati personali approvato con D.Lgs. 30 giugno 2003, n. 196;
- il Provvedimento Generale sulla videosorveglianza adottato dal Garante per la protezione dei dati personali in data 8 aprile 2010;
- la Direttiva 11 febbraio 2005 della Presidenza del Consiglio dei Ministri, Dipartimento della Funzione Pubblica;

Acquisito:

- il parere favorevole in ordine alla regolarità tecnica espresso dalla Responsabile del servizio, ai sensi degli artt. 49 e 147 bis del D. Lgs. nr. 267/2000;

Con la seguente votazione resa nei modi e termini di legge

- FAVOREVOLI : 13
- ASTENUTI : 3 (Miolla, Grieco e Di Trani)

DELIBERA

- di approvare, per le motivazioni sopra espresse, il Regolamento per la Videosorveglianza del Comune di Pisticci, che si allega al presente atto per farne parte integrante e sostanziale ad ogni effetto di legge, al fine di garantire il trattamento dei dati personali acquisiti mediante dispositivi di videosorveglianza, di varia tipologia, gestiti ed impiegati nel territorio comunale.
- di dichiarare l'entrata in vigore del presente Regolamento con l'esecutività della presente deliberazione di approvazione, secondo le leggi vigenti.
- di pubblicare la presente deliberazione all'Albo Pretorio on line per i termini di legge e il Regolamento sul sito internet del Comune permanentemente;
- di comunicare gli atti alla Prefettura di Matera – UTG; alla Questura di Matera, alla Procura della Repubblica presso il tribunale di Matera; al Commissariato di P.S. di Marconia; al Comando Compagnia C.C. di Pisticci e Stazione C.C. di Marconia e al Corpo di Polizia Locale.

**SUCCESSIVAMENTE
IL CONSIGLIO COMUNALE**

- Ritenuta l'indilazionabile urgenza di provvedere, con la seguente votazione resa ed espressa nei modi e termini di legge:FAVOREVOLI : 13 - ASTENUTI: 3 (Miolla, Grieco e Di Trani)

-

- DELIBERA

- Di dichiarare la presente deliberazione immediatamente eseguibile ai sensi dell'art. 134 -comma 4° - del T.U.E.L. approvato con D.Lgs. n. 267/2000.

IL PRESIDENTE DEL CONSIGLIO

Sodo Pasquale

IL SEGRETARIO GENERALE

Dott.ssa URICCHIO Grazia

CERTIFICATO DI PUBBLICAZIONE

(Art.124, D.Lgs. 267/2000)

N° 829 d'ordine

- E' stata affissa all'Albo pretorio Comunale il giorno 30-03-2023 per rimanervi quindici giorni consecutivi (art.124, D.Lgs. 267/2000);

Pisticci, li 30-03-23

IL SEGRETARIO GENERALE

Dott.ssa URICCHIO Grazia

IL SEGRETARIO GENERALE

Dott.ssa URICCHIO Grazia

CERTIFICATO DI ESECUTIVITA'

(Art.124, D.Lgs. 267/2000)

Che la presente deliberazione :

- E' divenuta esecutiva il giorno **09-04-23**
Perché dichiarata immediatamente eseguibile (art.134 , comma 4, del D.Lgs. n.267/2000)

E' copia conforme all'originale, da servire per uso amministrativo.

Pisticci, li 30-03-2023

IL SEGRETARIO GENERALE

Dott.ssa URICCHIO Grazia

COMUNE DI PISTICCI

REGOLAMENTO COMUNALE IN MATERIA DI VIDEOSORVEGLIANZA

Approvato con Deliberazione del Consiglio Comunale n. 7 del 27.03.2023

INDICE

- Art.1 - Premessa
- Art.2 - Norme di riferimento e principi generali
- Art.3 - Definizioni
- Art.4 - Finalità istituzionali dei sistemi di videosorveglianza
- Art.5 - Caratteristiche tecniche dell'impianto
- Art.6 - Informativa
- Art.7 - Valutazione di Impatto sulla protezione dei dati
- Art.8 - Titolare e funzionario designato del Trattamento dei dati
- Art.9 - Incaricati del Trattamento
- Art. 10 - Modalità di Raccolta e di Trattamento dei Dati
- Art. 11 - Sicurezza dei dati
- Art. 12 - Accesso ai dati
- Art. 13 - Diritti dell'interessato
- Art. 14 - Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale
- Art. 15 - Provvedimenti attuativi
- Art. 16 - Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali
- Art. 17 - Pubblicità del Regolamento
- Art. 18 – Entrata in vigore

CAPO I PRINCIPI GENERALI

Art. 1 Premessa

Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali; la videosorveglianza dà luogo, pertanto, a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.

Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza di varia tipologia gestiti e impiegati dal Comune di Pisticci nel territorio comunale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Art. 2 Norme di riferimento e principi generali

Il presente regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto di videosorveglianza cittadina e altre tipologie di videosorveglianza (fotrappole, body cam, dash cam e altri dispositivi idonei), attivati nel territorio del Comune di Pisticci.

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);
- 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 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 decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia”;
- D. 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”

EDPB (European Data Protection Board) Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video (adottate il 29 gennaio 2020).

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:

Principio di liceità – Il 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 e 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. Qualora non sia necessario individuare le persone, inoltre, 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 e 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. È 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:

- per «**dato personale**», qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- per «**trattamento**», qualsiasi operazione o insieme di attività, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- per «**banca dati**», il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;
- per «**profilazione**», qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- 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;
- per «**titolare del trattamento**», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- per «**incaricato del trattamento**», la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del funzionario designato al coordinamento delle attività e al controllo del trattamento;
- per «**interessato**», la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
- per «**terzo**», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il funzionario designato al coordinamento delle attività e al controllo del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del funzionario designato

al coordinamento delle attività e al controllo;

- 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;
- 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;
- per “**diffusione**”, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per “**dato anonimo**”, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

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 esicurezza 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 en.558/SICPART/421.2/70/224632 in data 2.3.2012;
- 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 Pisticci è precipuamente rivolto a garantire la sicurezza urbana che l'art. 1 del Decreto del Ministero 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 nonché 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 relative a elementi probatori in fattispecie di violazioni amministrative o penali potranno essere condivise con altre forze di Polizia competenti a procedere in tali casi di commissione di reati;
- c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e gli edifici pubbliche 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) per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche e accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
- h) monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
- i) 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.

Sarà possibile l'eventuale ripresa di immagini presso discariche comunali, solamente nel caso in cui non risulterà possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi e comunque nel rispetto del principio di minimizzazione dei dati. In tal caso, l'informativa agli interessati potrà essere fornita mediante affissione di cartelli informativi nei punti e nelle aree in cui si svolge la videosorveglianza, che contengano anche indicazioni su come e dove reperire un testo completo contenente tutti gli elementi di cui all'art. 13 del Regolamento.

Art. 5

Caratteristiche tecniche dell'impianto

Presso la sede municipale, del Corpo della Polizia Locale-Ufficio Videosorveglianza, è posizionato il sistema DVR ed il monitor per la registrazione, gestione e visione in diretta delle immagini riprese dalle telecamere.

I dati sono accessibili dal responsabile dell'Ufficio videosorveglianza della Polizia Locale che ha le chiavi di accesso del sistema, sia fisiche che software.

I dati sono estrapolabili Via Usb con pendrive o con Hdd portatile.

Le telecamere sono di tipologia IP (o analogiche con adattatore IP) e possono essere del tipo con tecnologia OCR, fisse (panoramiche e lettura targhe) o brandeggiabili (dome) a seconda degli obiettivi da perseguire. Nell'ipotesi in cui vengano utilizzate telecamere brandeggiabili saranno espressamente vietate per la ripresa di immagini/video su abitazioni private

Le telecamere IP sono collegate direttamente alla sala operativa sita in municipio presso gli Uffici della Polizia Locale tramite cavo di rete, fibra ottica o ponti radio, attraverso un'infrastruttura studiata per mappare il più possibile l'abitato.

Potranno, inoltre, essere utilizzati dal personale di Polizia Locale dispositivi denominati "fototrappola", "body cam", "dash cam" e altri dispositivi idonei, per l'uso del quale si applicherà il presente disciplinare di utilizzo.

Il sistema di videosorveglianza potrà essere implementato da dispositivi ritenuti idonei.

Le eventuali bodycam a disposizione della polizia locale potranno essere attivate solo in caso di necessità prestando la massima attenzione al rispetto del corretto trattamento dei dati personali (circolare del Ministero dell'Interno del 18-01-2022). Nello specifico le videocamere individuali verranno assegnate all'operatore di volta in volta e non sono configurabili dallo stesso. A fine turno le bodycam dovranno essere spente definitivamente ed i filmati esportati automaticamente dalla memoria locale nel momento del deposito del dispositivo sulla docking station. Le immagini dovranno essere conservate nel server situato nei locali della Polizia Locale per un periodo massimo di 6 mesi, salvo ulteriori esigenze investigative.

La scelta del posizionamento delle telecamere potrà essere effettuata di concerto tra l'Amministrazione Comunale e le principali Forze dell'Ordine.

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 quadro normativo di riferimento. In relazione ai principi di pertinenza e di non eccedenza già richiamati all'art. 2 del presente Regolamento, i sistemi informativi 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 ed opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 6 Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; 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** secondo quanto previsto dall'EDPB (European Data Protection Board) - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020 ed in ossequio al già richiamato Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010 che viene allegato al presente regolamento per frane parte integrante e sostanziale.

L'installazione dei cartelli contenenti l'informativa semplificata sulla videosorveglianza, dovrà avvenire nel rispetto del contenuto prescritto dagli artt. 13 e 14 del Regolamento UE 679/2016. 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 a 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. 7

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.

Art. 8

Titolare e funzionario designato del Trattamento dei dati

Il Titolare del trattamento dei dati è il Comune di Pisticci, al quale compete ogni decisione in ordine alle finalità e ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.

Il Responsabile dell'Ufficio videosorveglianza di Polizia Locale è 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 sull' 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:

- individua e nomina 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;
- provvede a rendere l'informativa "*minima*" agli interessati secondo quanto definito al precedente art. 6;
- verifica e controlla 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; garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;
- assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- adotta, 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;
- garantisce 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;
- assicura 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;
 - garantisce 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;
 - è 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;
 - assicura 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;
 - garantisce 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, necessaria a garantire il rispetto della normativa in materia di trattamento dei dati personali;
 - vigila sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Art. 9 Incaricati del Trattamento

Il funzionario designato al coordinamento delle attività e al controllo del trattamento dei dati procede a individuare, con proprio atto, le persone fisiche incaricate del trattamento dei dati, incaricate dell'utilizzazione degli impianti e, nei casi in cui risulti 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:

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 e 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 e integrato.

Art. 10

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 di ricezione, registrazione e visione

ubicata presso gli uffici della Polizia Locale. In questa sede 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.

Le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite (art. 5, paragrafo 1, lett. c) ed e), del Regolamento UE 676/2016). In base al principio di responsabilizzazione (art. 5, paragrafo 2, del Regolamento), spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Ciò salvo che specifiche norme di legge non prevedano espressamente determinati tempi di conservazione dei dati (si veda, ad esempio, l'art. 6, co. 8, del D.L. 23/02/2009, n. 11, ai sensi del quale, nell'ambito dell'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, "la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione"). In via generale, gli scopi legittimi della videosorveglianza sono spesso la sicurezza e la protezione del patrimonio. **Solitamente è possibile individuare eventuali danni entro uno o due giorni.**

Tenendo conto dei principi di minimizzazione dei dati e limitazione della conservazione, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve a rilevare atti vandalici) – cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione.

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. 11

Sicurezza dei dati

I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del precedente art. 10.

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 immagini 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-Fi, 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. 12 **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 necessità per il conseguimento delle finalità di cui all'art. 4 del presente Regolamento.

L'accesso alle immagini è consentito esclusivamente:

- a) al Titolare e 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 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. 13 **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) a 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.17GDPR, 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 dell'Ufficio Videosorveglianza del Corpo di Polizia Locale di Pisticci, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sulla home page del sito istituzionale dell'Ente).

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 dell'Ufficio Videosorveglianza del Corpo 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 personadi 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. 14

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. 15 **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. 16 **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.

Art. 17 **Pubblicità del Regolamento**

Copia del presente Regolamento sarà pubblicata all’albo pretorio e potrà essere reperita sul sito internet del Comune.

Art. 18 **Entrata in vigore**

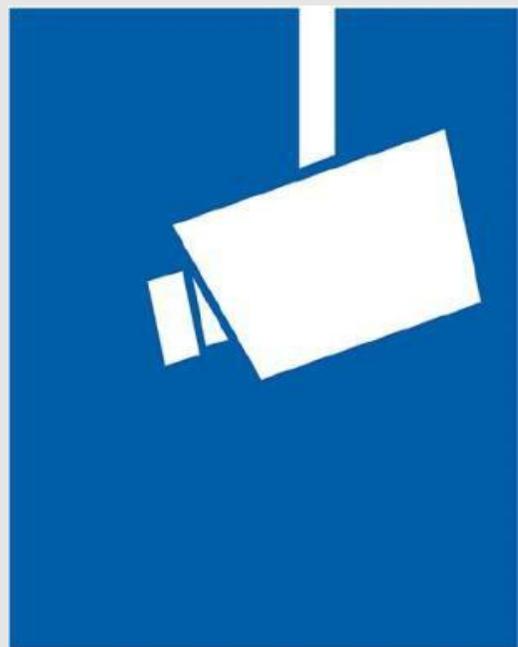
Il presente Regolamento entrerà in vigore con l’esecutività della deliberazione di approvazione, secondo le leggi vigenti.

Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.

MODELLO SEMPLIFICATO CARTELLO VIDEOSORVEGLIANZA

(EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020)

Per informazioni: www.garanteprivacy.it/faq/videosorveglianza



LA REGISTRAZIONE È EFFETTUATA DA

CONTATTI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (se applicabile):

.....

LE IMMAGINI SARANNO CONSERVATE PER UN PERIODO DI

FINALITÀ DELLA VIDEOSORVEGLIANZA

L'informativa completa sul trattamento dei dati è disponibile:

- presso i locali del titolare (reception, casse, ecc.)
- sul sito internet (URL)...
- altro

È POSSIBILE ACCEDERE AI PROPRI DATI ED ESERCITARE GLI ALTRI DIRITTI RICONOSCIUTI DALLA LEGGE RIVOLGENDOSI A