

CITTÀ DI GRAVINA IN PUGLIA

REGOLAMENTO COMUNALE
PER LA DISCIPLINA DELL'USO DELLE
IMMAGINI FORNITE DA IMPIANTI DI
VIDEOSORVEGLIANZA
IN AMBITO TERRITORIALE

Approvato con deliberazione del Consiglio Comunale n. 25 del 28/11/2022

INDICE GENERALE

CAPO I PRINCIPI GENERALI

- ART. 1** OGGETTO E NORME DI RIFERIMENTO
- ART. 2** DEFINIZIONI
- ART. 3** FINALITÀ DEL SISTEMA DI VIDEOSORVEGLIANZA - NORME DI RIFERIMENTO
- ART. 4** ALTRI SISTEMI DI VIDEOSORVEGLIANZA

CAPO II OBBLIGHI E ADEMPIMENTI PER I SOGGETTI ALLA GESTIONE DEL SISTEMA

- ART. 5** TITOLARE DEL TRATTAMENTO
- ART. 6** DESIGNATI PER IL TRATTAMENTO DEI DATI PERSONALI
- ART. 7** INCARICATI PER IL TRATTAMENTO DEI DATI PERSONALI E ALLA GESTIONE DELL'IMPIANTO DI VIDEOSORVEGLIANZA

CAPO III TRATTAMENTO DEI DATI PERSONALI MODALITÀ DI RACCOLTA, MISURE DI SICUREZZA E LIMITI ALLA UTILIZZABILITÀ DEI DATI

- ART. 8** ACCESSO AI SISTEMI E PAROLE CHIAVE
- ART. 9** DESCRIZIONE E ACCESSO AL SISTEMA DI VIDEOSORVEGLIANZA
- ART. 10** NORME PER LA GESTIONE DEL SISTEMA - MISURE DI SICUREZZA
- ART. 11** MODALITÀ DI RACCOLTA E REQUISITI DEI DATI PERSONALI.
- ART. 12** ACCERTAMENTI DI ILLECITI ED INDAGINI GIUDIZIARIE O DI POLIZIA
- ART. 13** OBBLIGHI DEGLI OPERATORI INCARICATI AL TRATTAMENTO
- ART. 14** INFORMAZIONI RESE AL MOMENTO DELLA RACCOLTA
- ART. 15** SICUREZZA DEI DATI
- ART. 16** CESSAZIONE DEL TRATTAMENTO DEI DATI
- ART. 17** LIMITI ALLA UTILIZZABILITÀ DI DATI PERSONALI
- ART. 18** DANNI CAGIONATI PER EFFETTO DEL TRATTAMENTO DI DATI PERSONALI.
- ART. 19** COMUNICAZIONE DEI DATI

CAPO IV DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI TUTELA AMMINISTRATIVA E GIURISDIZIONALE

- ART. 20** DIRITTI DELL'INTERESSATO
- ART. 21** PROCEDURA PER L'ACCESSO ALLE IMMAGINI,
- ART. 22** TUTELA

CAPO V DISPOSITIVI ELETTRONICI MOBILI

- ART. 23** UTILIZZO DI DISPOSITIVI ELETTRONICI MOBILI PER ATTIVITÀ DI PREVENZIONE E DI CONTROLLO.
- ART. 24** FINALITÀ DEL SISTEMA DI VIDEOSORVEGLIANZA MOBILE
- ART. 25** ELENCO DELLE POSSIBILI E NON ESAUSTIVE ZONE VIDEOSORVEGLIATE
- ART. 26** NORME DI RINVIO

CAPO VI DISPOSIZIONI FINALI

- ART. 27** RINVII ED ABROGAZIONI
- ART. 28** ENTRATA IN VIGORE E PUBBLICAZIONE

CAPO I
PRINCIPI GENERALI

ART. 1- OGGETTO E NORME DI RIFERIMENTO

1. Il presente regolamento disciplina il trattamento dei dati personali realizzato mediante il "sistema di videosorveglianza" cittadina ed altre tipologie di videosorveglianza (fototrappole, body cam, dash cam, telecamere mobili, Drone, ZTL, lettura targhe) attivati nel territorio del Comune di Gravina in Puglia.
2. 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:
 - a. **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.
 - b. La videosorveglianza comunale, pertanto, è consentita senza necessità di consenso da parte degli interessati.
 - c. **Principio di necessità** - In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), GDPR, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.
 - d. **Principio di proporzionalità** - La raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza, Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento. Nell'uso delle apparecchiature volte a riprendere, per 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.
 - e. **Principio di finalità** - Ai sensi dell'art. 5, Paragrafo 1, lett. b), GDPR, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana che il DM Interno 05/08/2008 definisce come il "bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."

3. Per tutto quanto non è dettagliatamente disciplinato nel 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".
- Legge 7 marzo 1986, n. 65, (Legge quadro ordinamento polizia Locale);
- D.P.R. 24 luglio 1977, n. 616;
- D.Lgs. 31 marzo 1998, n. 112 - (conferimento compiti e funzioni amministrative dello Stato alle Regioni ed agli Enti locali);
- D.Lgs. 18 agosto 2000, n. 267 - (TUEL testo unico delle leggi sull'ordinamento degli enti locali);
- Legge 24 luglio 2008, n. 125 - (misure urgenti in materia di sicurezza pubblica);
- Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana;
- Legge 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale;
- Circolari del Ministero dell'Interno n.558/A/421.2/70/456 in data 8 febbraio 2005, n. 558/A421.2/70/195860 in data 6 agosto 2010 e n. 558/SICPART/421.2/70/224632 in data 2.3.2012;
- nonché da funzioni istituzionali previste dallo Statuto e dai Regolamenti comunali.

ART. 2 - DEFINIZIONI

Ai fini del presente Regolamento si intende:

- a. 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;

- b. 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;
- c. 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;
- d. 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;
- e. 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;
- f. 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;
- g. 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;
- h. per «**interessato**», la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
- i. 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;
- 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 «**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;
- l. per «**diffusione**», il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- m. per «**dato anonimo**», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
- n. per «**Designato**», il cosiddetto "soggetto designato" di cui all'art 2- quaterdecies della dlgs. 101/2018, il cui titolo recita "Attribuzione di funzioni e compiti a soggetti designati"

ART. 3 - FINALITÀ DEL SISTEMA DI VIDEOSORVEGLIANZA - NORME DI RIFERIMENTO

1. Le finalità che il Comune di Gravina in Puglia intende perseguire con l'attività di videosorveglianza è quello della sicurezza urbana e rispetto del Codice della Strada, si collocano nella cornice normativa relativa allo svolgimento delle funzioni istituzionali previste dalla Legge
2. Gli impianti di videosorveglianza, in sintesi, sono finalizzati alla sicurezza urbana e rispetto del Codice della Strada come segue:
 - a) a prevenire 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", così come delineato dal Decreto Ministro Interno del 5 agosto 2008;
 - b) alla verifica e controllo del traffico in tempo reale per prevenire situazioni di pericolo o intralcio per la circolazione ed in modo che sia in ogni caso salvaguardata la sicurezza stradale, con conseguente più razionale e pronto impiego delle risorse umane;
 - c) alla tutela degli immobili di proprietà dell'Amministrazione Comunale per prevenire eventuali atti predatori, di vandalismo o danneggiamento;
 - d) al controllo di determinate aree sensibili rilevanti sotto il profilo della prevenzione generale e della sicurezza;
 - e) ad attività di prevenzione e di controllo, con impianti di videosorveglianza fissi e/o mobili, volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose, nonché monitoraggio del rispetto delle disposizioni concernenti modalità e tipologia di deposito dei rifiuti.
 - f) attività di protezione civile sul territorio comunale;
Potranno inoltre essere installati sul territorio comunale impianti finalizzati alla rilevazione del transito dei veicoli, alle aree pedonali all'uso costituite, per finalità di prevenzione e vigilanza.
3. L'impianto di videosorveglianza esterna sul territorio cittadino è gestito dal Comune di Gravina in Puglia presso la centrale operativa del Comando del Corpo di Polizia Locale. Presso l'eventuale centrale operativa interforze, tramite un apposito protocollo d'intesa, potranno essere collocate le postazioni per la visione in tempo reale delle immagini riprese dalle telecamere e per gli accessi al sistema di videosorveglianza secondo le modalità descritte nel Capo III.
4. Le finalità del suddetto impianto sono altresì conformi alle funzioni istituzionali demandate dalle leggi e dai regolamenti ai Comandi Interforze che ne faranno richiesta in relazione ai rispettivi ordinamenti speciali. Le immagini, visionate presso il Comando del Corpo della Polizia Locale ed eventualmente presso la centrale operativa Interforze costituiscono altresì uno strumento di prevenzione e di razionalizzazione dell'azione delle pattuglie operanti sul territorio comunale e sono finalizzate ad attuare uno stretto raccordo operativo tra le forze di Polizia Locale e Statale. L'impianto è destinato anche all'osservazione diretta da remoto, gli apparati infatti, consentono di osservare una determinata area quando, in presenza di particolari eventi, se ne ravvisi l'esigenza. Il sistema effettua una vera e propria attività di vigilanza su persone e beni, sostituendo, in tutto o in parte, la presenza umana sul posto.
5. L'attività di videosorveglianza raccoglie esclusivamente 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 sono e saranno quindi stabilite in modo conseguente.
6. L'impianto di videosorveglianza non può essere utilizzato, in base all'art. 4 dello Statuto dei lavoratori (Legge 300 del 20 maggio 1970) per finalità di controllo a distanza dell'attività lavorativa dei dipendenti dell'Amministrazione Comunale, di altre amministrazioni pubbliche o di altri datori di

lavoro, pubblici o privati. L'impianto di videosorveglianza non può essere utilizzato per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.

ART. 4 ALTRI SISTEMI DI VIDEOSORVEGLIANZA

1. Il personale della Polizia Locale può utilizzare, per i servizi individuati dall'Amministrazione comunale e dal Responsabile della Struttura organizzativa, dispositivi ulteriori di ripresa, anche a tutela della sicurezza dell'operatore stesso, come Body Cam (telecamere posizionate direttamente sulle divise degli operatori di P.L.), Dash Cam fisse a bordo di veicolo di servizio, Droni, in conformità delle indicazioni dettate dal Garante per la protezione dei dati personali, con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi, ed il cui trattamento dei dati viene ricondotto a dati personali direttamente correlati all'esercizio di compiti di polizia, di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria.
2. In relazione all'utilizzo di Body Cam, Dash Cam, Droni e Fototrappole, il Responsabile della Struttura organizzativa, sulla base delle reali necessità operative di tutela dell'operatore, nonché della necessità di assicurare le fonti di prova anche per fini probatori e di polizia giudiziaria, istruisce gli operatori di Polizia Locale, con indicazione delle casistiche di attivazione di tali strumenti in funzione dei servizi espletati, dei soggetti eventualmente autorizzati a disporre l'attivazione, delle operazioni autorizzate in caso di emergenza e di ogni altra misura organizzativa e tecnologica necessaria alla corretta e legittima gestione di detti dispositivi.
3. Il trattamento informatico dei dati acquisiti con strumenti Body Cam, Dash Cam, Droni e fototrappole, avviene secondo quanto disciplinato dall'accordo contrattuale stipulato con il fornitore della strumentazione ed in ogni caso in ottemperanza alle normative tecniche di attuazione (es. Regolamento Mezzi aerei a pilotaggio remoto di ENAC, ecc.) ed alle norme in tema di protezione dei dati personali, ponendo in essere misure tecniche e organizzative adeguate per la protezione degli stessi.
4. Dovranno essere implementati ed adottati tutti gli eventuali adempimenti di natura giuslavoristica a protezione del personale dipendente soggetto al trattamento dei dati acquisiti con tali strumenti.

CAPO II

OBBLIGHI E ADEMPIMENTI PER I SOGGETTI GESTORI DEL SISTEMA

ART. 5 - TITOLARE DEL TRATTAMENTO

1. Il Comune di Gravina in Puglia, nella sua qualità di titolare del trattamento dei dati personali, rientrante nel campo di applicazione del presente regolamento, adempie agli obblighi di notificazione preventiva al Garante per la protezione dei dati personali, qualora ne ricorrano i presupposti, ai sensi e per gli effetti degli artt. 37 e 38 del Codice.
2. Il titolare del trattamento provvede altresì a richiedere la verifica preliminare prima di mettere in funzione sistemi di telecamere nei casi individuati nell'art. 3.2.1. del Provvedimento in materia di videosorveglianza - 8 Aprile 2010 (Gazzetta Ufficiale n. 99 del 29 Aprile 2010) e s.m.e i e attraverso un'analisi di rischio e impatto come previsto all'articolo 35 del GDPR (General Data Protection Regulation è la normativa europea in materia di protezione dei dati) : "Quando un tipo di trattamento, prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto

dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi". A tale proposito la normativa prevede che non vanno comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardino immagini conservate temporaneamente per esclusive finalità di sicurezza pubblica o di tutela delle persone e del patrimonio.

3. Il titolare provvede al fine di rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati, a esporre informativa sul trattamento dati attraverso cartelli semplificativi, benché non obbligatoria, laddove l'attività di videosorveglianza sia espletata ai sensi dell'art. 53 del Codice assicurandosi che sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati.

ART. 6 - DESIGNATI PER IL TRATTAMENTO DEI DATI PERSONALI.

1. L'organo apicale dell'ente individua i designati del trattamento dei dati personali, in base alle rispettive competenze come disciplinato dall'art. 2 Quaterdieces del D. Lgs. n. 101/18 che prevede l'attribuzione di funzioni e compiti specifici nell'ambito del proprio assetto organizzativo.
2. Sono designati al trattamento dei dati il Comandante del Corpo di P.L. ed, in assenza e/o impedimento di quest'ultimo, il Referente pro-tempore del comandante (in assenza di vice comandante), in relazione al complesso di operazioni concernenti la ripresa delle immagini, la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, l'eventuale diffusione, la cancellazione e la distribuzione di dati dagli stessi soggetti pubblici fruibili e trattati.
3. Con riferimento al punto precedente, oltre alle figure ivi previste, potranno essere incaricati altri appartenenti al Corpo di P.L., per tutte o solamente per determinate attività, con esclusiva delega del comandante ed anche per periodi determinati.
4. Gli incaricati devono rispettare pienamente quanto previsto, in tema di trattamento dei dati personali e delle misure di sicurezza, dalle leggi vigenti e dalle disposizioni previste dal presente regolamento.
5. I soggetti designati ed il personale incaricato, osservano le disposizioni previste dal presente regolamento compatibilmente con i rispettivi ordinamenti speciali, nonché in relazione alle disposizioni e agli accessi al sistema di videosorveglianza consentiti dal titolare.
6. I soggetti designati ed il personale incaricato procedono al trattamento attenendosi alle istruzioni impartite dal titolare, il quale vigila sulla puntuale osservanza del presente regolamento e delle disposizioni di legge.
7. I soggetti designati ed il personale incaricato custodiscono le chiavi per l'accesso ai locali del sistema centralizzato di videosorveglianza, nonché le parole chiave per l'utilizzo dei sistemi.
8. Lo svolgimento del predetto servizio non comporterà alcuna indennità aggiuntiva per designati e incaricati.
9. In particolare, i soggetti designati ed il personale incaricato 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 Responsabile del Trattamento dei Dati ed al Responsabile della Protezione dei Dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

ART. 7 - INCARICATI PER IL TRATTAMENTO DEI DATI PERSONALI E ALLA GESTIONE DELL'IMPIANTO DI VIDEOSORVEGLIANZA,

1. Il Comandante, tra gli appartenenti al Corpo di P.L., può incaricare altri soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati, o per specifiche esigenze, potrà essere incaricato altro personale interno previa formazione e sottoscrizione di precise istruzioni e obblighi del trattamento.
2. La gestione operativa dell'impianto di videosorveglianza è riservata al personale del Corpo di P.L. Il Comandante può autorizzare altro personale, in casi particolari, debitamente motivati, per specifiche attività e per periodi anche limitati.
3. Con l'atto di nomina ai singoli incaricati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dell'impianto. In particolare gli incaricati sono istruiti al corretto uso dei sistemi e formati circa le disposizioni della normativa di riferimento e del presente regolamento.
4. Il Comandante individua e nomina, ove opportuno, gli incaricati ("responsabili del trattamento esterni") ai sensi dell'art. 28 del GDPR (UE) 2016/679 (Regolamento del Parlamento e del Consiglio del 27/04/16) e la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR). Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
5. Il Comandante, a suo insindacabile giudizio, può revocare la nomina di qualsiasi altro soggetto autorizzato/incaricato/designato.

CAPO III

TRATTAMENTO DEI DATI PERSONALI MODALITÀ DI RACCOLTA, MISURE DI SICUREZZA E LIMITI ALLA UTILIZZABILITÀ DEI DATI

ART. 8 - ACCESSO AI SISTEMI E PAROLE CHIAVE.

1. L'accesso ai sistemi è esclusivamente consentito esclusivamente ai soggetti autorizzati/incaricati/designati, come individuati negli articoli precedenti
2. I predetti soggetti saranno dotati di propria password complessa di almeno 10 caratteri per accesso al sistema e dovranno attenersi al piano di sicurezza adottato dall'Ente.

ART. 9 - DESCRIZIONE E ACCESSO AL SISTEMA DI VIDEOSORVEGLIANZA.

1. Il sistema di videosorveglianza si compone di una rete di comunicazione dati, basata su tecnologie miste e di telecamere dislocate sul territorio comunale per riprendere luoghi pubblici (quand'anche, per esigenze tecnico-operative, collocate su proprietà private) e connesse alla centrale operativa. Il sistema ed i relativi apparati sono isolati a livello logico, non sono interconnessi con altri sistemi, archivi o banche dati, né accessibili da altre periferiche non facenti parte dello stesso sistema, ad eccezione di eventuali collegamenti con le centrali operative delle Forze dell'Ordine.
2. L'accesso al sistema è esclusivamente consentito al responsabile e agli incaricati come indicato nel presente regolamento, secondo le seguenti modalità:
 - a. la gestione delle telecamere avviene in modo automatico dal sistema, tranne per quelle in fase di utilizzo da parte dell'operatore abilitato;
 - b. accesso tecnico: in caso di necessità per manutenzione e assistenza, possono accedere alla visualizzazione delle immagini sia il soggetto esterno (appaltatore del servizio che per esperienza, capacità ed affidabilità fornisce idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati) in qualità di installatore/manutentore dell'impianto, che il personale tecnico appositamente incaricato dallo stesso; le attività possono essere eseguite per lavori di manutenzione ordinaria e/o straordinaria, od in presenza di segnalazioni di anomalie/verifiche di funzionalità del sistema o dei suoi singoli apparati;
3. In merito alle postazioni di visualizzazione differita e duplicazione delle immagini registrate, l'accesso al sistema avviene secondo le seguenti modalità:
 - a. accesso utente: l'accesso avviene esclusivamente su pre-definite postazioni ad esso dedicate e posizionate presso la centrale operativa del Corpo di Polizia Locale e quella eventualmente posta presso la centrale operativa interforze. L'incaricato alla consultazione delle immagini registrate si autentica al sistema mediante opportune credenziali di autenticazione; una volta autenticato, l'incaricato accede all'area di gestione, attraverso la quale può visualizzare gestire le immagini trasmesse dalle telecamere o può accedere all'archivio digitale nel quale è possibile ricercare, salvare e duplicare immagini o filmati per i fini istituzionali secondo quanto previsto nel presente regolamento;
 - b. accesso tecnico: in caso di necessità, manutenzione e assistenza, il soggetto esterno installatore/manutentore, abilitato al servizio tecnico mediante personale appositamente incaricato, può accedere al sistema di videoregistrazioni ed alla visualizzazione delle immagini registrate esclusivamente per le suddette necessità e nel rispetto degli obblighi di segretezza e riservatezza.

ART. 10 - NORME PER LA GESTIONE DEL SISTEMA - MISURE DI SICUREZZA.

1. I dati raccolti mediante il sistema di videosorveglianza sono protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
2. In particolare, gli uffici comunali competenti e i soggetti nominati responsabili del sistema integrato adottano le seguenti specifiche misure tecniche ed organizzative di sicurezza:

1. CENTRALE OPERATIVA DEL CORPO DI POLIZIA LOCALE:

- l'accesso al sistema di controllo della videosorveglianza in esercizio permanente, è consentito al responsabile e agli incaricati. È consentito l'accesso temporaneo di soggetti accreditati e incaricati di servizi e funzioni rientranti nei compiti istituzionali del Comune di Gravina in Puglia. È consentito, altresì, l'accesso al personale addetto alla manutenzione degli impianti e alla pulizia dei locali, i cui nominativi devono essere comunicati per iscritto al Comando e annotati sul "registro degli accessi", ove istituito. Eventuale accesso di altri e diversi soggetti deve essere appositamente autorizzato per iscritto dal designato responsabile interno per il trattamento dei dati personali;
- l'accesso al locale della centrale operativa della Polizia Locale, ove sono presenti i monitor di controllo della videosorveglianza con accensione permanente, deve essere provvisto di una idonea porta con serratura che permette l'accesso ai soggetti accreditati e di un climatizzatore che permette di mantenere la temperatura idonea per il locale de quo, la cui installazione, a cura del responsabile del settore tecnico è preventiva alla messa in funzione dell'impianto de quo;
- l'accesso ai locali che ospita il server della videosorveglianza deve essere provvisto di una porta idonea con serratura;
- l'armadio che contiene il gruppo server della videosorveglianza deve avere una idonea serratura di sicurezza;
- l'accesso al locale che ospita il server della videosorveglianza è consentito a soggetti accreditati.

2. ALTRI SOGGETTI, OVE PREVISTO, DEL SISTEMA INTEGRATO:

- Il responsabile del trattamento, ai sensi dell'art. 5 del presente regolamento, adotta idonee e specifiche misure tecniche ed organizzative di sicurezza in relazione ai rispettivi ordinamenti speciali, fermo restando che i monitor devono essere posizionati in modo idoneo, in ambienti ove l'accesso è controllabile ed in modo da non consentire la visione diretta ed immediata delle immagini a soggetti estranei al Corpo di P.L..
- L'accesso informatico al sistema di videosorveglianza deve essere tracciato ed archiviato elettronicamente, nonché annotato sul "registro degli accessi", ove istituito.

3. MISURE TECNICHE DI SICUREZZA GENERALE DEL SISTEMA DI VIDEOSORVEGLIANZA:

- nessuna postazione di videosorveglianza può accidentalmente cancellare ovvero distruggere quanto registrato nel server;
- il software di gestione deve governare l'accesso al sistema di videosorveglianza con credenziali di autenticazione abilitanti;
- la cronologia degli eventi di accesso al sistema videosorveglianza deve essere archiviata elettronicamente per almeno sei mesi;
- le credenziali per gli accessi al sistema di videosorveglianza devono essere disattivate in caso di mancato utilizzo per un periodo pari o superiore a sei mesi o in caso di perdita dell'incarico che consente al soggetto l'accesso al sistema di videosorveglianza;
- tutti gli apparati esterni, tra il giorno 11 ed il giorno 15 e tra il giorno 26 e la fine di ciascun mese solare, devono essere periodicamente monitorati, personalmente dal titolare dell'appalto di manutenzione, a cui compete segnalare, tempestivamente, ogni anomalia o manomissione all'U.T.C. e, per conoscenza, al Comando P.L;
- La Polizia Locale, quotidianamente, dovrà verificare la funzionalità di tutte le telecamere e segnalarne all'U.T.C. eventuali anomalie. Tali segnalazioni dovranno essere annotate in apposito registro;

- L'Ufficio Tecnico Comunale, cui compete la gestione tecnica permanente degli impianti, autorizzerà la ditta incaricata della manutenzione (compresi la pulizia e la manutenzione i cartelli per assicurare l'informativa ex art. 13 del GDPR citato richiamata dal provvedimento del Garante per la Protezione dei dati Personali dell'08/04/10), salvo che per le attività che non comportano ulteriori o nuove spese o che rientrano nell'eventuale canone fisso di manutenzione, per le quali la ditta incaricata dovrà provvedere automaticamente senza alcuna necessaria comunicazione preventiva seppur non preclusa.
- Il Comando di Polizia Locale che utilizza il sistema di videosorveglianza gestisce i dati ed evade le richieste, di detti dati, da parte di Corpi di polizia per le sole indagini di polizia giudiziaria ed a seguito di richiesta formale del rispettivo Comando e a seguito di notifica di consegna/comunicazione dei dati medesimi. Il Comando di P.L. potrà segnalare eventuali anomalie e richiedere per determinati siti l'intervento di manutenzione urgente.
- la telecomunicazione ed il trasporto delle informazioni potrà avvenire con sistema di crittografia avente idonee chiavi di cifratura che escludono ogni accesso abusivo.

ART. 11 - MODALITÀ DI RACCOLTA E REQUISITI DEI DATI PERSONALI.

1. I dati personali oggetto di trattamento sono:
 - a) trattati in modo lecito e secondo correttezza;
 - b) raccolti e registrati per le finalità di cui al presente Regolamento e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni compatibili con tali scopi;
 - c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
 - d) conservati principalmente in base ad una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità ex art. 35 par. 7 lett. b) GDP 2016/679 - per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per i quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito nel presente articolo e secondo una valutazione del Comando di P.L., sulla scorta, di volta in volta, delle esigenze di monitorare determinati siti oggetto di osservazione per fini investigativi del Comando di P.L. o nell'interesse di altri Corpi di polizia.
2. I dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza, installate sul territorio comunale in relazione alle esigenze di prevenzione generale, ordine e sicurezza pubblica. Il numero delle telecamere potrà essere eventualmente ampliato, secondo gli sviluppi futuri del sistema, mediante approvazione di apposite deliberazioni della Giunta Comunale e/o altri provvedimenti amministrativi. Le telecamere consentono, tecnicamente, riprese video diurne/notturne a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.
3. Il Titolare del trattamento dei dati personali si obbliga a non effettuare delle riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa saranno raccolti da un sistema centralizzato posto in un locale situato presso il Comune di Gravina in Puglia. In questa sede le immagini saranno registrate su supporto digitale da un sistema appositamente predisposto e visualizzate in tempo reale su monitor posti presso la centrale operativa della Polizia Locale.
4. Gli apparati di ripresa e i software devono funzionare con dei "preset" (pre-settaggio in ordine a posizionamento, rotazione, durata) secondo le indicazioni del Comando di P.L. o con altri accorgimenti idonei ad evitare, durante la cosiddetta funzione in tour automatico, la ripresa dell'interno delle finestre degli edifici. Sia la ditta incaricata dell'installazione che quella

incaricata della manutenzione saranno responsabili dei predetti accorgimenti; atteso che a causa di cattivo funzionamento, di manomissione, di danneggiamento ovvero di modifica dello stato dei luoghi si potrà rendere necessario adottare appositi accorgimenti atti ad evitare violazioni del codice della privacy.

5. Le immagini videoregistrate sono conservate, per un tempo adeguato alle specifiche finalità di rilevazione, presso il server di sistema che consente di aderire alle finalità indicate nel presente Regolamento nonché a specifiche richieste investigative dell'autorità giudiziaria o della polizia giudiziaria. I tempi di conservazione verranno modulati secondo le finalità e basi giuridiche valutate da Analisi del Rischio e Impatto Privacy, come indicato dall'Art. 35 del (UE) GDPR 2016/679.

Art. 12 – ACCERTAMENTI DI ILLECITI ED INDAGINI GIUDIZIARIE O DI POLIZIA.

1. Nell'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 (7) 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 Responsabile potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai predetti (7) giorni previa richiesta al Garante per la protezione dei dati personali che, a seguito di verifica preliminare, potrà rilasciare parere favorevole.
2. 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.
3. Alle immagini raccolte, ai sensi del presente articolo, possono accedere, per l'espletamento delle relative indagini, solo gli appartenenti all'Amministrazione Giudiziaria, le persone da essi espressamente autorizzate e gli organi di Polizia.
4. Qualora gli organi di Polizia, nello svolgimento dei loro compiti istituzionali, necessitino di copia delle riprese effettuate, devono registrare tale necessità, previa apposita, preventiva richiesta al Comando di Polizia Locale, nell'apposito registro, così come previsto nel presente Regolamento.
5. Nel caso in cui gli organi di Polizia o della Polizia Locale, 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.

Fatta eccezione per fatti gravi o di particolare rilevanza per indagini giudiziarie, l'accesso potrà essere effettuato dalle ore 08.00 alle ore 20.00 dei giorni feriali, secondo le modalità sopra indicate.

ART. 13 - OBBLIGHI DEGLI OPERATORI INCARICATI AL TRATTAMENTO

1. L'utilizzo del brandeggio da parte degli operatori incaricati al trattamento deve essere conforme ai limiti indicati nel presente regolamento.
2. L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolga nei luoghi pubblici, aperti al pubblico o soggetti a pubblico passaggio. Esso non è ammesso per sorvegliare luoghi privati. Eventuali riprese di dettaglio dei tratti somatici delle persone devono essere funzionali alle finalità istituzionali dell'impianto.

3. Fatti salvi i casi di richiesta degli interessati al trattamento, di cui al presente Regolamento, i dati registrati possono essere riesaminati accedendo all'area dell'archivio digitale, nel limite del tempo ammesso per la conservazione, solo in caso di effettiva necessità per il conseguimento delle finalità di cui al presente Regolamento.
4. La mancata osservanza degli obblighi previsti dal 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.

ART. 14 - INFORMAZIONI RESE AL MOMENTO DELLA RACCOLTA

1. Il Comune di Gravina in Puglia, in ottemperanza a quanto disposto dal GDPR, è obbligato ad installare un'adeguata segnaletica permanente nelle strade e nelle piazze in cui sono posizionate le telecamere. I cartelli hanno caratteristiche tali da essere chiaramente visibili in ogni condizione di illuminazione ambientale ed in orario notturno, come previsto dalla Normativa Vigente.
2. Il Comune di Gravina in Puglia è obbligato a comunicare alla comunità cittadina l'attivazione dell'impianto di videosorveglianza, l'eventuale incremento dimensionale dell'impianto e l'eventuale successiva cessazione per qualsiasi causa dello stesso mediante appositi strumenti informativi e di comunicazione locale.

ART. 15 - SICUREZZA DEI DATI

1. I dati personali oggetto di trattamento sono custoditi ai sensi e per gli effetti degli artt. 8, 9 e 10 del presente regolamento.
2. I dati sono protetti da idonee e preventive misure di sicurezza, individuate con documentazione tecnica rilasciata dalla ditta installatrice, riducendo al minimo i rischi di distruzione, di perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
3. Vanno comunque assicurate alcune misure, cosiddette minime, obbligatorie anche dal punto di vista penalistico.
4. I dati personali oggetto di trattamento sono custoditi nella centrale operativa situata presso la sede della Polizia Locale. Alla sala dedicata al Servizio e ubicata in un luogo chiuso al pubblico, possono accedere esclusivamente il responsabile, gli incaricati del trattamento dei dati e gli autorizzati. Non possono accedervi altre persone se non sono accompagnate da soggetti autorizzati e per esclusivi motivi di servizio o di manutenzione. L'utilizzo dei videoregistratori impedisce di rimuovere il disco rigido su cui sono memorizzate le immagini.

ART. 16 - CESSAZIONE DEL TRATTAMENTO DEI DATI

1. In caso di cessazione per qualsiasi causa di un trattamento, i dati personali sono:
 - a) distrutti;
 - b) eccezionalmente conservati in relazione a procedimenti connessi alle finalità di cui all'art. 3 del presente regolamento.
2. Nel caso il supporto debba essere sostituito per eccessiva usura, sarà distrutto in modo da renderlo inutilizzabile e che non possano essere recuperati i dati in esso presenti.

ART. 17 - LIMITI ALLA UTILIZZABILITÀ DI DATI PERSONALI

1. La materia è disciplinata dal GDPR in materia di protezione dei dati personali.
2. Tutti gli accessi alla visione saranno documentati mediante 'annotazione in un apposito "registro degli accessi" (cartaceo e/o informatico), conservato nei locali della centrale operativa della Polizia Locale, nel quale sono riportati ad opera degli incaricati.
 - a) la data e l'ora dell'accesso;
 - b) l'identificazione di chi accede;
 - c) i dati per i quali si è svolto l'accesso;
 - d) gli estremi e la motivazione dell'autorizzazione all'accesso;
 - e) le eventuali osservazioni dell'incaricato anche in ordine all'eventuale irregolare funzionamento;
 - f) richiesta di copia del video da estrapolare e motivazione;
 - g) la sottoscrizione del medesimo.

ART. 18 - DANNI CAGIONATI PER EFFETTO DEL TRATTAMENTO DI DATI PERSONALI.

1. La materia è regolamentata per l'intero dal GDPR di cui, alla data di stesura del presente regolamento, è vigente il n. 2016/679.

ART. 19 - COMUNICAZIONE DEI DATI

1. La comunicazione dei dati personali da parte del titolare 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 e solo esclusivamente per lo svolgimento delle funzioni istituzionali e può essere iniziata se è decorso il termine di preventiva comunicazione al Garante di cui all'art. 39 c. 2 del Codice.
2. È sempre ammessa la comunicazione dei dati all'Autorità Giudiziaria e alla polizia giudiziaria per le finalità di accertamento o repressione di reati.
3. Non si considera comunicazione, ai sensi e per gli effetti del presente articolo, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal responsabile.
4. È in ogni caso fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, per finalità di difesa o di sicurezza dello Stato.
5. La comunicazione dei dati ed in ogni caso l'estrazione e la duplicazione delle immagini registrate salvo i casi di cui ai commi 2 e 4 del presente articolo, può avvenire solo a seguito di autorizzazione di volta in volta rilasciata dal responsabile al trattamento specificatamente incaricato dal titolare.

CAPO IV

DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI

TUTELA AMMINISTRATIVA E GIURISDIZIONALE

ART. 20 - DIRITTI DELL'INTERESSATO

1. In relazione al trattamento dei dati personali l'interessato ha diritto di ottenere l'indicazione da parte del responsabile al trattamento specificatamente incaricato dal titolare:
 - a) dell'esistenza di trattamenti di dati che possono riguardarlo;
 - b) degli estremi identificativi del titolare e del responsabile;
 - c) delle finalità e modalità del trattamento cui sono destinati i dati;

- d) la conferma dell'esistenza o meno di dati personali che lo riguardano e la comunicazione de 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.
2. L'interessato ha diritto di ottenere la cancellazione, 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.
 3. L'interessato ha diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.
 4. I diritti dell'interessato sono esercitati dietro presentazione di apposita istanza che non potrà essere reiterata, dallo stesso soggetto, se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi.
 5. Il responsabile del trattamento darà esito all'istanza senza ritardo e comunque non oltre 30 giorni dalla data di ricezione della richiesta, ovvero 30 giorni previa comunicazione all'interessato se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo.
 6. 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.
 7. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.
 8. L'istanza di cui al presente articolo può essere trasmessa al titolare o al responsabile anche mediante lettera raccomandata, posta elettronica certificata (PEC), o mail firmata digitalmente. Il responsabile dovrà provvedere, in merito, entro e non oltre i termini di cui al comma 5 del presente articolo.
 9. 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. 21 - ACCESSO AI FILMATI

Al di fuori dei diritti dell'interessato, l'accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente.

Ogni richiesta deve essere specifica, formulata per iscritto, motivata ed indirizzata al designato del trattamento dei dati competente entro 3 giorni dall'evento. Non è consentito fornire ai cittadini copia delle immagini, salvo il rispetto della L. 241/90.

Per finalità di indagine, l'Autorità giudiziaria e la Polizia giudiziaria possono richiedere ed acquisire copia delle immagini in formato digitale.

Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, copia delle riprese in formato digitale può essere richiesta ed acquisita dall'organo di polizia stradale che ha proceduto ai rilievi ed in capo al quale è l'istruttoria relativa all'incidente.

Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'art. 391-quater c.p.p., può richiedere ed acquisire copia delle riprese in formato digitale previo pagamento delle relative spese individuate con apposita deliberazione di giunta comunale sulle tariffe di accesso ai documenti amministrativi.

Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al designato del trattamento che i filmati siano conservati oltre i termini di legge, per essere messi a disposizione dell'organo di polizia procedente. Spetta all'organo di polizia procedente presentare richiesta di acquisizione dei filmati. Tale richiesta deve pervenire entro tre mesi dalla data dell'evento, decorsi i quali i dati non saranno ulteriormente conservati.

In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dal designato del trattamento dei dati deve annotare le operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, con lo scopo di garantire la genuinità dei dati stessi.

Possono essere divulgate immagini provenienti dagli impianti di videosorveglianza, previa anonimizzazione di ogni dato che consenta l'identificazione dei soggetti.

ART. 22 – TUTELA

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto per Legge.
2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt.4-6 L. 241/90, è il responsabile del trattamento dei dati personali, così come individuato dall'art. 5 del presente regolamento.

CAPO V

DISPOSITIVI ELETTRONICI MOBILI

ART. 23 - UTILIZZO DI DISPOSITIVI ELETTRONICI MOBILI PER ATTIVITÀ DI PREVENZIONE E DI CONTROLLO.

1. Al fine di garantire una maggiore sicurezza urbana, nonché per migliorare l'attività di prevenzione e di controllo del territorio, potranno essere posizionate telecamere mobili nei punti ritenuti "sensibili" di volta in volta individuati dal Comando di Polizia Locale.
2. Il presente capo garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di un impianto di videosorveglianza mobile nel territorio del Comune di Gravina in Puglia, gestito e utilizzato dalla Polizia Locale, si svolga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale e soltanto per lo svolgimento delle funzioni istituzionali.
3. Garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento
4. La telecamera di cui al precedente comma 1, registra e memorizza in modo autonomo le immagini videoriprese e sarà opportunamente segnalata dall'informativa di cui al presente Regolamento.
5. Le immagini registrate verranno trattate secondo quanto predisposto dal D.P.I.A. (Data Protection Impact Assessment).

ART. 24 - FINALITÀ DEL SISTEMA DI VIDEOSORVEGLIANZA MOBILE.

1. Le finalità del suddetto impianto, del tutto conformi alle funzioni istituzionali demandate al Comune di Gravina in Puglia, sono:
 - a. l'attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale;
 - b. la ricostruzione della dinamica di atti vandalici o azioni di teppismo, per permettere un pronto intervento della Polizia Locale e delle Forze dell'Ordine a tutela del patrimonio pubblico;

- c. l'individuazione dei cittadini che commettono atti non conformi quali l'abbandono improprio dei rifiuti o modalità di conferimento degli stessi, diverse da quelle previste nell'apposito regolamento;
2. Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali, rilevati mediante le riprese video e fotografiche che, in relazione ai luoghi di installazione delle videocamere, interesseranno i soggetti ed i mezzi di trasporto che transiteranno nelle aree videosorvegliate.
 3. L'attività di videosorveglianza raccoglie esclusivamente 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 quindi stabilite in modo conseguente.
 4. L'uso dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate all'apposita normativa vigente in materia di "privacy".

CAPO VI DISPOSIZIONI FINALI

ART. 27 - RINVII ED ABROGAZIONI.

1. Per quanto non disciplinato dal presente regolamento si rinvia alle norme legislative e regolamentari, ai provvedimenti attuativi delle medesime, alle decisioni del Garante e ad ogni altra normativa, speciale, generale, nazionale e comunitaria in materia di protezione e trattamento dei dati personali nell'ambito della videosorveglianza.
2. Ogni altra disposizione antecedente nonché contraria o incompatibile con il presente regolamento in materia di videosorveglianza del territorio comunale si deve intendere abrogata.
3. I contenuti del presente Regolamento si intendono aggiornati con la normativa in vigore all'epoca del trattamento dei dati personali se in contrasto con la stessa.

ART. 28 - ENTRATA IN VIGORE E PUBBLICAZIONE.

1. Il presente Regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della relativa deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite.
2. Copia del regolamento è pubblicato all'Albo Pretorio Comunale online e sul sito internet del Comune di Gravina in Puglia.