



COMUNE DI MONOPOLI

Provincia di Bari

Via Garibaldi n.6, C.A.P. 70043 Monopoli – Italia

DISCIPLINARE PER LA REGOLAMENTAZIONE ED IL CORRETTO UTILIZZO DEL SISTEMA PROFESSIONALE DI VIDEOSORVEGLIANZA INDOSSABILE (BODYCAM) PER RIPRESA DI VIDEO E DI IMMAGINI NEI SERVIZI A RISCHIO OPERATIVO DELLA POLIZIA LOCALE E DELLE FOTOTRAPPOLE PER MONITORAGGIO IN AMBIENTI A RISCHIO ALTO DI ABBANDONO RIFIUTI

INDICE

Art. 1	Premessa	3
Art. 2	Normativa applicabile	3
Art. 3	Ambito di applicazione del trattamento dei dati	4
Art. 4	Finalità del trattamento dei dati	4
Art. 5	Base Giuridica	7
Art. 6	Notificazione preventiva al Garante della Privacy	7
Art. 7	Titolare del Trattamento	7
Art. 8	Responsabile della Protezione dei dati	8
Art. 9	Designato al Trattamento	9
Art. 10	Persona Autorizzata al Trattamento	10
Art. 11	Responsabile della Gestione Tecnica dei dispositivi di videosorveglianza	12
Art. 12	Modalità di raccolta e conservazione dati acquisiti con impiego di bodycam ..	12
Art. 13	Modalità di raccolta e conservazione dati acquisiti con impiego di fototrappole 13	
Art. 14	Valutazione d'impatto sulla protezione dei dati personali e consultazione preventiva con l'Autorità di Controllo	16
Art. 15	Periodo di conservazione dei dati	16
Art. 16	Requisiti dei dati personali per impiego di bodycam	17
Art. 17	Obblighi degli operatori di Polizia Locale	18
Art. 18	Accertamenti di illeciti ed indagini giudiziarie o di polizia	18
Art. 19	Diritti dell'interessato	19
Art. 20	Sicurezza Dei Dati	20
Art. 21	Modalità di autenticazione e credenziali	21
Art. 22	Diritti dell'interessato	23
Art. 23	Comunicazione dei dati	23
Art. 24	Accertamento di illeciti e indagini delle autorità giudiziarie e/o di polizia	24
Art. 25	Cessazione del trattamento dei dati	25
Art. 26	Limiti alla utilizzabilità di dati personali	25
Art. 27	Danni cagionati per effetto del trattamento di dati personali	25
Art. 28	Destinatari dei dati personali trattati	25
Art. 29	Violazione Dei Dati Personali	26
Art. 30	Tutela Amministrativa e Giurisdizionale	27
Art. 31	Tutela dei dati personali	27
Art. 32	Pubblicità del disciplinare	27
Art. 33	Soppravvenienza di nuove disposizioni normative	28
Art. 34	Entrata in vigore e successive modifiche del regolamento	28

Art. 1 Premessa

1. Le immagini e le videoriprese qualora rendano possibile l'identificazione diretta o indiretta di persone, costituiscono dati personali. La ripresa di videosorveglianza, le immagini e i video raccolti con dispositivi in uso alla Pubblica Amministrazione comportano un trattamento di dati personali ed incidono sul diritto delle persone alla propria riservatezza.
2. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, cioè che si realizza a distanza mediante dispositivi per le riprese video collegati o meno ad un centro di controllo e coordinamento.
3. Con il presente disciplinare si garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione dei sistemi di videosorveglianza indossabili sulla divisa degli operatori della Polizia Locale, c.d. "*bodycam*" gestiti e impiegati dal Comune di Monopoli nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; garantisce, altresì, i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento, avuto riguardo anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico.
4. Ai fini delle definizioni di cui al presente Disciplinare si deve fare riferimento all'art. 4 del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali e all'art 2 del D.lgs. n. 51/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Art. 2 Normativa applicabile

1. Per tutto quanto non dettagliatamente disciplinato dal presente Disciplinare, si rinvia a quanto disposto dal:
 - ✓ **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";
 - ✓ **Decreto Legislativo 30 giugno 2003, n.196** recante il "Codice in materia di protezione dei dati personali" come da ultimo modificato con Decreto Legislativo 10 agosto 2018, n. 101;
 - ✓ **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”;

- ✓ **DPR n. 15 del 15.01.2018**
“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”;
- ✓ **Decreto Legislativo del 18 maggio 2018, n. 51**
“Attuazione della direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione

quadro 2008/977/GAI del Consiglio.

- ✓ **Decreto Ministero dell'Interno 05 agosto 2008**
Incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione. (GU Serie Generale n.186 del 09-08-2008)
- ✓ **Provvedimento del Garante del 8 aprile 2010 (G.U. n. 99 del 29/04/2010)** per la Protezione dei Dati Personali in materia di Videosorveglianza

Art. 3 Ambito di applicazione del trattamento dei dati

1. Il trattamento dei dati personali effettuato tramite l'utilizzo di bodycam rientra nell'ambito di applicazione del Decreto Legislativo 18 Maggio 2018, n. 51 che in attuazione della Direttiva n. 680/2016 regola il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse da parte sia dell'autorità giudiziaria, sia delle forze di polizia.

Art. 4 Finalità del trattamento dei dati

1. Il trattamento dei dati personali effettuato tramite l'utilizzo di fototrappole e di bodycam da parte degli operatori in servizio della Polizia Locale rientra nell'ambito di applicazione del:

- ✓ Decreto Legislativo 18 Maggio 2018, n. 51 che in attuazione della Direttiva n. 680/2016 regola il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse da parte sia dell'autorità giudiziaria, sia delle forze di polizia.
 - ✓ Codice di Procedura Penale art. 354 comma 1 specifica che gli ufficiali e gli agenti di Polizia Giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero. Mentre il comma 2 specifica che se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose.
2. Il predetto trattamento pertanto è finalizzato, in modo del tutto conforme alle funzioni istituzionali demandate al Comune di Monopoli,
- dalle disposizioni legislative e regolamentari in vigore, alla tutela dell'ordine e della sicurezza pubblica, alla prevenzione, all'accertamento o alla repressione dei reati ed in particolare:
- ✓ prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse da parte sia dell'autorità giudiziaria, sia delle forze di polizia
 - ✓ attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale;
 - ✓ prevenzione e contrasto dei fenomeni di criminalità (sicurezza urbana, come definita dall'art. 4 del D.L. 20.02.2017, n. 14 e ss.mm.);
 - ✓ ricostruzione, in tempo reale, della dinamica di atti vandalici o fatti criminosi o azioni di teppismo nei luoghi pubblici di principale frequentazione, anche a tutela del patrimonio pubblico;
 - ✓ vigilanza sul pubblico traffico per consentire l'immediata adozione di idonee contromisure;
 - ✓ acquisire elementi probatori in fattispecie di violazioni penali o amministrative anche in danno agli agenti del Corpo di Polizia Locale;

- ✓ verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;
 - ✓ accertare violazioni alle norme del Codice della Strada ai sensi dell'art. 201 comma 1-bis lettere e), f), g), g-bis) del D. Lgs. 30 aprile 1992, nr. 285 e ss.mm., in conformità a quanto disposto dal Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza del 8 aprile 2010 (G.U. n. 99 del 29/04/2010) che richiama altresì la prassi ed il quadro normativo di settore riguardante talune violazioni del Codice della strada;
 - ✓ attività di monitoraggio e contrasto al fenomeno dell'abbandono incontrollato di rifiuti;
 - ✓ attività di controllo e ispettive, nonché sanzionatorie e di tutela in sede amministrativa e/o giudiziaria;
 - ✓ prevenire e reprimere fenomeni di degrado urbano e svolgere controlli volti ad accertare e sanzionare violazioni delle norme in materia ambientale e delle disposizioni del regolamento per la gestione integrata dei rifiuti urbani, qualora risultino difficili o inefficaci l'attuazione di altre misure.
 - ✓ nel caso si tratti di fatti di rilievo penale, ma ne sia dato formalmente atto ai sensi degli artt. 348, 354 e 357 del c.p.p.
 - ✓ ogni qualvolta sia necessario compiere rilievi video e fotografici per l'accertamento delle violazioni amministrative, ai sensi dell'art. 13 della Legge 689/1981.
- In particolare, lo scopo dell'acquisizione dei dati è la documentazione di specifiche attività preventive o repressive di fatti di reato e situazioni dalle quali possano derivare minacce per l'ordine e la sicurezza pubblica o un pericolo per la vita e l'incolumità dell'operatore, e allo stesso tempo il rafforzamento della sicurezza obiettiva e di quella individualmente percepita da cittadini e operatori, grazie alla elevata capacità deterrente/dissuasiva delle bodycam.
3. L'utilizzo delle bodycam comporterà esclusivamente il trattamento di dati personali, rilevati mediante le riprese video, in relazione ai luoghi ove presta servizio il personale di Polizia Locale, e interesseranno i soggetti ed i mezzi di trasporto che transiteranno nell'area.
 4. In attuazione del principio di proporzionalità e dei criteri di pertinenza e non eccedenza, i sistemi di videosorveglianza sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed

evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti.

5. La possibilità di disporre in tempo reale di dati ed immagini costituisce un ulteriore strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell'ambito delle proprie competenze istituzionali sul territorio comunale in stretto raccordo con le altre Forze dell'Ordine; attraverso tali strumenti si persegue l'intento di tutelare la popolazione ed il 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, nelle contrade e negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.

Art. 5 Base Giuridica

1. La base giuridica del trattamento eseguito con le bodycam e con le fototrappole, ai sensi dell'articolo 6, comma 1, lettera e) del Regolamento (UE) 2016/679 è rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento ed il Comandante del Comando di Polizia Locale.
2. Il trattamento è altresì basato sull'interesse legittimo volto alla tutela

della sicurezza del personale e alla tutela del patrimonio comunale del Titolare del trattamento (art. 6 comma 1, lettera f) del Regolamento (UE) 2016/679.

3. Le bodycam e le fototrappole non potranno essere utilizzate, 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. Inoltre, per l'utilizzo delle stesse, non è previsto il consenso da parte degli interessati, rientrando il trattamento tra i compiti di interesse pubblico di cui è investito il titolare.
4. Le bodycam e le fototrappole non potranno altresì essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.

Art. 6 Notificazione preventiva al Garante della Privacy

1. Dal 25 maggio 2018 cessa l'obbligo di notificazione previsto dall'art. 37, comma 4, del decreto legislativo n. 196/2003.

Art. 7 Titolare del Trattamento

1. Il Comune di Monopoli, rappresentato ai fini previsti dal GDPR dal Sindaco pro tempore (o suo delegato), è il Titolare

del trattamento dei dati personali (di seguito Titolare), acquisiti mediante l'utilizzo delle bodycam o delle fototrappole e raccolti in banche dati elettroniche o archivi cartacei, come definiti dall'art. 4 par. 1, n. 6 del GDPR. Il Sindaco può delegare le relative funzioni a Dirigenti di Area Organizzativa in possesso di adeguate competenze, quali Designati al trattamento dati.

2. Il Titolare dei dati personali acquisiti mediante l'utilizzo dei sistemi di videosorveglianza:
 - a. definisce le linee organizzative per l'applicazione della normativa di settore;
 - b. effettua le notificazioni al Garante per la protezione dei dati personali laddove necessarie;
 - c. nomina i designati al trattamento, i responsabili della gestione tecnica degli impianti di videosorveglianza ed i responsabili del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti e/o dispositivi di videosorveglianza, impartendo istruzioni ed assegnando compiti e responsabilità;
 - d. detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo dei sistemi e/o dispositivi di videosorveglianza;
 - e. vigila sulla puntuale osservanza delle disposizioni impartite.

3. Il Titolare, per i dati acquisiti mediante l'utilizzo delle bodycam o delle fototrappole, adotta le misure tecniche e organizzative, quali la crittografia, la minimizzazione, la pseudonimizzazione, etc., fin dalla fase di progettazione del servizio di videosorveglianza con bodycam e fototrappole (privacy by design) per garantire che siano trattati per impostazione predefinita (privacy by default) solo i dati necessari per la specifica finalità di trattamento;

Art. 8 Responsabile della Protezione dei dati

1. Il titolare del trattamento nomina un Responsabile della protezione dei dati in ossequio all'art. 37 del GDPR.
2. Il Responsabile per la protezione dei dati adempie alle proprie funzioni in piena autonomia, indipendenza ed in assenza di conflitti di interesse.
3. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
 - a. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente disciplinare nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

- b. sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
 - c. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;
 - d. cooperare con l'autorità di controllo;
 - e. fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
4. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Art. 9 Designato al Trattamento

1. Il Designato al trattamento dei dati con funzioni di responsabilità (di seguito Designato) nominato dal Sindaco con atto formale, nonché Comandante del Corpo di Polizia Locale di Monopoli, è preposto al trattamento dei dati contenuti nelle banche dati acquisiti mediante l'utilizzo delle bodycam e/o delle fototrappole e assume la responsabilità del trattamento dei dati personali rilevati, sul quale gravano i doveri di vigilanza e di adozione delle precauzioni.
2. I Designati effettuano il trattamento nel rispetto della normativa vigente in materia di protezione dei dati personali, ivi incluso il profilo della sicurezza, e delle disposizioni del presente disciplinare.
3. I Designati effettuano il trattamento attenendosi alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle proprie disposizioni ed istruzioni.
4. Il Designato del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza:
 - a. collaborano per l'evasione delle richieste di esercizio dei diritti degli interessati;
 - b. custodiscono le chiavi di accesso ai locali delle centrali di controllo e le chiavi dei locali e degli armadi nei quali sono custoditi i supporti contenenti le registrazioni;

- c. assicurano che le persone autorizzate 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 operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
 - d. garantiscono la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale individuato quale persone autorizzate al trattamento con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;
 - e. vigilano sul rispetto da parte delle persone autorizzate degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.
5. Nella situazione di affidamento all'esterno della gestione di una banca dati, il Designato provvede a nominare responsabile esterno del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

Art. 10 Persona Autorizzata al Trattamento

- 6. Il Comandante il Corpo di Polizia Locale di Monopoli, delegato dal Sindaco, provvede alla designazione con atto formale di nomina, delle Persone Autorizzate al trattamento dei dati, ossia il personale interno afferente alle singole strutture in cui si articola la propria Area Organizzativa Comunale che sono preposti al trattamento dei dati contenuti negli archivi esistenti nelle articolazioni organizzative di loro competenza e nello specifico gli Agenti di Polizia Locale che tratteranno i dati contenuti nelle banche dati acquisiti mediante l'utilizzo delle bodycam o delle fototrappole.
- 7. Le persone autorizzate sono nominate tra gli appartenenti al Corpo di Polizia Locale ed eventualmente agli altri servizi comunali che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
- 8. Le persone autorizzate effettuano il trattamento attenendosi scrupolosamente alle istruzioni impartite dal Titolare e dai Designati del trattamento dei dati personali.
- 9. Nell'ambito delle persone autorizzate, sono designate, con l'atto di nomina, i soggetti ai quali sono affidate la custodia e la conservazione delle chiavi di accesso ai locali delle centrali di controllo e delle chiavi dei locali e degli

armadi nei quali sono custoditi i supporti contenenti le registrazioni.

10. In particolare, le persone autorizzate devono:

- a. 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;
- b. 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;
- c. mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
- d. 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;
- e. evitare di creare banche dati nuove senza autorizzazione espressa del Designato al trattamento dei dati;
- f. mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;
- g. conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
- h. fornire al Designato del trattamento dei dati ed al Responsabile della Protezione dei dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo;
- i. Le persone autorizzate al trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del Designato.
- j. L'utilizzo degli apparecchi di ripresa da parte delle persone autorizzate al trattamento dovrà essere conforme ai limiti indicati dal presente disciplinare come eventualmente modificato e integrato.

Art. 11 Responsabile della Gestione Tecnica dei dispositivi di videosorveglianza

1. Il Comandante del Corpo di Polizia Locale può nominare, uno o più Responsabili della gestione tecnica degli impianti e/o dispositivi di videosorveglianza di cui al presente disciplinare. La nomina è effettuata con contratto o altro atto giuridico equipollente secondo la normativa nazionale, nel quale sono analiticamente specificati i compiti affidati al responsabile.
2. I Responsabili della gestione tecnica degli impianti e/o dispositivi di videosorveglianza:
 - a) gestiscono la manutenzione degli impianti di videosorveglianza urbana;
 - b) accedono al software di gestione degli impianti di videosorveglianza ed ai relativi dati registrati;
 - c) assegnano e custodiscono le credenziali di accesso necessarie per l'utilizzo degli impianti di videosorveglianza.

Art. 12 Modalità di raccolta e conservazione dati acquisiti con impiego di bodycam

1. Le bodycam, dotate di memoria interna fissa caratterizzata disco rigido da 32 Gb, sono contraddistinte da un numero

seriale che dovrà essere annotato in apposito registro recante il giorno, l'orario, la qualifica e nominativo del dipendente che firmerà la presa in carico e la restituzione, le eventuali note di servizio, e conservato nella centrale operativa.

2. La bodycam, all'atto della consegna ai singoli operatori di Polizia Locale in servizio, non dovrà contenere alcun dato archiviato.
3. L'operatore di Polizia Locale in caso di necessità attiverà la bodycam, su ordine dell'Ufficiale o del Capopattuglia, in relazione all'evolversi degli scenari che facciano presupporre criticità e provvederà a cessare le riprese al termine degli stessi. Le riprese potranno essere riattivate ogni qualvolta l'operatore stesso ne ravvisi la necessità. Quando concretamente possibile, l'Agente di Polizia Locale e/o il Capopattuglia informerà l'interlocutore della registrazione video/audio in atto con una comunicazione del tipo "*Avvio Registrazione*".
4. Al termine del servizio gli operatori di Polizia Locale interessati, previa compilazione di un apposito modello di consegna, affideranno tutta la documentazione video realizzata al designato del trattamento, il quale provvederà personalmente, o tramite persona da lui delegata, al controllo della strumentazione e del corretto scarico dei dati. Nel predetto modello di consegna oltre ai dati dell'operatore

di Polizia Locale, al numero di identificazione della bodycam, al tipo di servizio, ed all'intervallo di tempo di registrazione, vengono specificate una dei seguenti motivi della registrazione:

- ✓ Attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale.
 - ✓ Ricostruzione, in tempo reale, della dinamica di atti vandalici o fatti criminosi o azioni di teppismo nei luoghi pubblici di principale frequentazione, anche a tutela del patrimonio pubblico.
 - ✓ Attività di monitoraggio e contrasto al fenomeno dell'abbandono incontrollato di rifiuti.
 - ✓ Vigilanza sul pubblico traffico per consentire l'immediata adozione di idonee contromisure.
 - ✓ Attività di polizia giudiziaria.
5. I dati registrati con la bodycam vengono salvati, da parte del Comandante e/o dal Responsabile della gestione tecnica, all'interno di una cartella archiviata in un hard disk esterno a stato solido (di seguito SSD) con crittografia integrata da algoritmo di crittografia sicuro, dotato di protezione password, rendendo i dati memorizzati più sicuri.

Art. 13 Modalità di raccolta e conservazione dati acquisiti con impiego di fototrappole

1. Il Comando di Polizia Locale di Monopoli, al fine di scoraggiare e prevenire l'incivile e diffuso fenomeno dell'abbandono di rifiuti e la creazione di "microdiscariche" sparse nel territorio comunale, fa ricorso ai sistemi mobili di foto-video ripresa denominati "Fototrappole". Queste si innescano a seguito di qualsiasi movimento di esseri umani o animali in una certa regione di interesse monitorata da un sensore ad alta sensibilità di movimento a infrarossi passivo, per poi scattare foto o video clip. Una volta che il movimento dell'uomo o dei veicoli viene rilevato, la fotocamera digitale sarà attivata e quindi automaticamente scatterà foto o video in base alle impostazioni programmate.
2. Le fototrappole vengono installate in zone del territorio comunale maggiormente soggette al fenomeno dell'abbandono di rifiuti, allo scopo di monitorare dette aree e per l'individuazione delle persone e anche le targhe dei veicoli dai quali vengono abbandonati i rifiuti.
3. Le riprese filmate e l'estrapolazione dei fotogrammi per l'accertamento degli illeciti ambientali potranno riguardare solo le immagini concernenti violazioni contemplate nel Testo Unico Ambientale, D.lgs. 152/ 2006, (utilizzo abusivo di aree impiegate come

discariche di materiali e di sostanze pericolose con riflessi penali e/o amministrativi a seconda delle norme violate e delle relative sanzioni stabilite: D.lgs. 152/2006 artt. 256, 255) sia le violazioni amministrative alle disposizioni emanate dal Comune (corretto conferimento dei rifiuti).

4. Le fototrappole caratterizzate da un telaio robusto che lo protegge da cadute accidentali fino a 2 metri, garantiscono la sicurezza tramite un lettore di impronte digitale integrato, protezione opzionale con password basata sul sistema di crittografia hardware AES a 256 bit e sono dotate di una scheda di archiviazione di massa da 64 Gb (di seguito SD).
5. Per consentire il funzionamento corretto e il controllo continuo della fotocamera, il comando può nominare un operatore esterno, incaricato con opportuno verbale in qualità di ausiliario di polizia giudiziaria (Art.348, comma 4, 357, 359 c.p.p.), che con frequenza massima di max 62 ore dalla prima installazione o dall'ultimo ripristino, deve provvedere al setup alla sostituzione delle batterie e della memoria interna.
6. L'operatore provvedere ad estrarre la scheda SD conservandola opportunamente in apposito contenitore protettivo custodendola attentamente per garantire la massima protezione da eventuali furti, manomissioni e danneggiamenti da terzi sino all'arrivo in sede presso il Comando di Polizia Locale.
7. La fototrappola è caratterizzata da un contenitore costruito completamente in acciaio, tagliato al laser, verniciato e mimetico che consente di proteggerla da furti e manomissioni non autorizzate. La fototrappola viene corredata da doppio lucchetto di sicurezza che permette la chiusura del contenitore metallico dove all'interno è ivi alloggiata e allo stesso tempo l'ancoraggio del contenitore ad un palo/albero. La chiave viene opportunamente conservata dall'operatore di Polizia Locale riposta in ufficio in una cassetta di sicurezza compilando l'apposito verbale di gestione chiavi ad uso dei lucchetti di sicurezza fototrappole.
8. La fototrappola viene installata solitamente su pali della luce nei siti segnalati dagli Enti preposti al Controllo della Polizia Locale. Il fissaggio avviene tramite staffe ancorate al palo con relativo contenitore dove all'interno viene alloggiata la fototrappola, al termine dell'installazione viene posizionata in modo tale da video sorvegliare solo l'area interessata all'abbandono ad un'altezza non inferiore ai 3/4 metri, protetta da lucchetti di sicurezza.
9. Alternativa utilizzata laddove non sono presenti pali della luce, alberi dove l'altezza media si riduce di circa un metro ma la sicurezza non implora in quanto la colorazione mimetica della

fototrappola, del contenitore ivi compreso il lucchetto, si integrano nella vegetazione mimetizzandosi. Questi accorgimenti servono per la protezione della parte hardware e la protezione dei dati presenti all'interno della memoria di archiviazione di massa da parte di tentato furto o danneggiamenti.

10. L'installazione degli apparati di cui al presente articolo è subordinata alla collocazione di apposita informativa, ai sensi dell'art. 13 del GDPR, mediante l'apposizione del cartello che deve essere collocato prima del raggio di azione della fototrappola, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti.

11. Sarà data massima visibilità all'installazione di cartelli segnaletici riportanti la dicitura del tipo: "Area sottoposta a videosorveglianza". Gli stessi saranno posizionati nei siti contemporaneamente all'installazione delle fototrappeole. Sarà cura dell'operatore eseguire degli scatti fotografici per la dimostrazione dei cartelli installati.

12. La modalità di sbobinatura ed analisi delle immagini presenti nella scheda SD avvengono nella seguente modalità:

- ✓ l'operatore nella stessa giornata del ripristino della camera e della sostituzione della scheda SD ha l'obbligo della sbobinatura ed analisi dei file registrati;

- ✓ I file della scheda SD vengono visualizzati su un computer dedicato e protetto in rete;
- ✓ durante la sbobinatura vengono archiviati solo ed esclusivamente i file oggetto di abbandoni da parte di sconosciuti con autoveicoli, motociclo, cicli o appiedati;
- ✓ la restante parte dei file non inerenti agli abbandoni vengono immediatamente cancellati formattando la scheda SD;
- ✓ I file oggetto di abbandoni vengono inseriti all'interno di una cartella riportante la data ed il luogo interessato e vengono archiviati in un hard disk esterno SSD a stato solido con crittografia integrata da algoritmo di crittografia sicuro, dotato di protezione password, rendendo i dati memorizzati più sicuri;
- ✓ In caso di nomina di operatore esterno al Corpo (ausiliario di P.G.), questi con cadenza quindicinale consegna all'ente di pertinenza i file oggetto di abbandono e formatta i dati presenti all'interno della scheda SD alla presenza di un Pubblico Ufficiale e viene redatto un verbale di distruzione di file, e sottoscritto dalle parti;
- ✓ Su apposito registro informatizzato si terrà conto del numero delle immagini estrapolate, del luogo e della data di acquisizione delle stesse. La conservazione dei dati, su apposito supporto informatico accessibile solo agli operatori ed

organi di Polizia, avverrà sino a conclusione del processo sanzionatorio.

con altri dati tali da provocare pregiudizio per gli interessati

Art. 14 Valutazione d'impatto sulla protezione dei dati personali e consultazione preventiva con l'Autorità di Controllo

1. Il Comune di Monopoli nella sua qualità di titolare del trattamento dei dati personali adempie all'obbligo previsto dall'art. 35 Reg. Eu 2016/679 in tema di valutazione d'impatto sulla protezione dei dati personali.
2. Il titolare del trattamento consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati ai sensi del suindicato art. 35 presenti un rischio elevato per i diritti e le libertà delle persone fisiche, in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; osserva in ogni caso integralmente quanto previsto dall'art. 36 del medesimo regolamento comunitario.
3. Per le bodycam, il Titolare rileva che tali sistemi si limitano a riprendere gli interventi di polizia, dal punto di vista dell'operatore stesso che indossa la telecamera, senza altre associazioni con altri dati tali da provocare pregiudizio per gli interessati
4. Per le fototrappole, il Titolare rileva che tali sistemi si limitano a una lettura delle targhe, senza altre associazioni

Art. 15 Periodo di conservazione dei dati

5. In caso di registrazione di riprese in occasione di situazioni di presunto pericolo per l'ordine e la sicurezza pubblica poi non concretizzatosi, le immagini stesse dovranno essere tempestivamente cancellate, in quanto il loro ulteriore trattamento risulterebbe estraneo alle finalità di cui al Decreto Legislativo 51/2018.
6. Le immagini video e/o audio videoregistrate sono conservate per un tempo non superiore a sette giorni, fatte salve speciali esigenze di ulteriore conservazione nei limiti e con le modalità stabilite al punto 3.4. del provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010, ed in modo particolare, in relazione ai dati relativi all'accertamento:
 - ✓ dei reati saranno conservati sino ai termini di cui all'articolo 10 comma 3 lett. U del D.P.R. 15 gennaio 2018, n. 15.
 - ✓ delle violazioni amministrative dovranno essere conservati fino alla conclusione del procedimento sanzionatorio o all'eventuale definizione dei rimedi giurisdizionali avverso gli atti sanzionatori.

7. L'accesso ai dati raccolti e conservati viene consentito solo per eventi che necessitano di indagine, su richiesta dell'Autorità giudiziaria e per quelli che hanno originato una responsabilità civile, amministrativa e penale dell'Azienda e del relativo personale.

Art. 16 Requisiti dei dati personali per impiego di bodycam

1. I dati personali oggetto di trattamento devono essere:
 - ✓ trattati in modo lecito e secondo correttezza, effettuati con i sistemi di ripresa in questione e rispettare i principi espressi dal D.lgs. 30 giugno 2003, n. 196 così come modificato dal D.lgs. 101/18, nonché dal Reg. UE 27 aprile 2016, n. 2016/679/UE (cd. GDPR) e dal D.lgs. 18 maggio 2018, n. 51;
 - ✓ essere pertinenti, completi e non eccedenti le finalità per le quali risultano essere raccolti, ovvero successivamente trattati, nonché conservati per un periodo non superiore a sette giorni in una forma che consenta l'identificazione dell'interessato, fatte salve speciali esigenze di ulteriore conservazione. Al termine del tempo stabilito le riprese dovranno essere cancellate come specificato al precedente articolo 10;
 - ✓ trattati, con riferimento alla finalità di cui al precedente articolo 4, con modalità rivolte a salvaguardare

l'anonimato anche successivamente alla fase della raccolta, atteso che tali immagini registrate potrebbero contenere dati di carattere personale.

2. I trattamenti di cui al D.lgs. 51/2018 debbono rispettare i principi di cui agli articoli 5 e 6 del GDPR; tra questi, in particolare, quelli secondo cui i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato.
3. Il sistema di ripresa video con le bodycam dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza di concrete e reali situazioni di pericolo di turbamento dell'ordine e della sicurezza pubblica.
4. In caso di registrazione di riprese in occasione di situazioni di presunto pericolo per l'ordine e la sicurezza pubblica poi non concretizzatosi, le immagini stesse dovranno essere tempestivamente cancellate, in quanto il loro ulteriore trattamento risulterebbe estraneo alle finalità di cui al Decreto Legislativo 51/2018.
5. Le registrazioni video delle unità di ripresa saranno raccolte da una stazione di monitoraggio e controllo, collocata presso la centrale operativa del Comando di Polizia Locale. In questa sede le immagini saranno trasferite direttamente su un hard disk

esterno a stato solido con crittografia integrata da algoritmo di crittografia sicuro, dotato di protezione password, rendendo i dati memorizzati più sicuri, per permetterne la conservazione a norma. Le immagini videoregistrate sono conservate per un tempo non superiore a sette giorni come specificato al precedente art. 14.

Art. 17 Obblighi degli operatori di Polizia Locale

1. All'inizio del servizio d'istituto l'operatore di Polizia Locale sub consegnatario dovrà indossare la bodycam, agganciata alla divisa attraverso gli idonei attacchi, indicando la data, l'ora e il numero della bodycam presa in carico.
2. Al termine del servizio il predetto operatore di Polizia Locale sub consegnatario dovrà rimettere nella base di ricarica la bodycam, provvedendo ad annotare nell'apposito registro l'ora di riconsegna. Successivamente verranno scaricate le immagini eventualmente registrate da parte del Comandante e/o dal Responsabile del servizio tecnico come specificato al precedente art. 12 comma 5), provvedendo alla conservazione a norma delle stesse con le modalità indicate nell'art. 14.
3. L'utilizzo delle bodycam da parte degli operatori e delle persone autorizzate al trattamento dovrà essere conforme alle finalità all'art. 4.

4. L'utilizzo del brandeggio da parte degli operatori e degli incaricati al trattamento dovrà essere conforme ai limiti indicati nel presente regolamento e dalle norme in materia.
5. L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolge nei luoghi pubblici mentre esso non è ammesso nelle proprietà private.
6. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente art. 14, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 e a seguito di regolare autorizzazione.
7. La mancata osservanza degli obblighi previsti al 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. 18 Accertamenti di illeciti ed indagini giudiziarie o di polizia

1. In caso di rilevazioni di immagini di fatti concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza, della tutela ambientale e/o del patrimonio pubblico, la persona autorizzata o il Designato provvederà a darne comunicazione, senza ritardo, all'Autorità competente, provvedendo,

allo stesso tempo, alle conservazioni delle immagini su appositi supporti.

2. 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.
3. Qualora gli organi di Polizia, nello svolgimento dei loro compiti istituzionali, necessitino una copia delle riprese effettuate, devono presentare un'istanza scritta circostanziata e motivata indirizzata al Comandante del Comando di Polizia Locale.

Art. 19 Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:
 - a) di chiedere in ogni momento all'interessato Ente la conferma dell'esistenza di trattamenti che possono riguardarlo nonché l'accesso ai propri dati personali, la rettifica degli stessi qualora non siano veritieri, nonché la loro cancellazione
 - b) di richiedere la limitazione del trattamento che lo riguarda, e può opporsi allo stesso laddove sia esercitato in modo illegittimo.
 - c) l'apposita istanza relativa all'esercizio dei sopracitati diritti

può essere presentata o al Titolare del trattamento o al Responsabile della protezione dei dati (R.P.D. / D.P.O) designato. Tale istanza deve essere corredata di ogni informazione e documentazione utile a dimostrare il legittimo interesse del richiedente.

2. Ai sensi degli artt. 12, 13 e 14 del Reg. EU 2016/679, per le richieste di cui al comma 1) let. a) del presente articolo, le informazioni fornite ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da n. 15 a 22 e n. 34 della medesima norma comunitaria sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:
 - a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
 - b) rifiutare di soddisfare la richiesta.
3. Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.
4. 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.

5. 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.
6. La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti alla persona istante identificabile e può comprendere eventuali dati riferiti a terzi, solo nei limiti previsti dalla Legge. A tal fine la verifica dell'identità del richiedente deve avvenire mediante esibizione o allegazione di un documento di riconoscimento che evidenzia un'immagine riconoscibile dell'interessato.
7. Le istanze di cui al presente articolo possono essere trasmesse al titolare del trattamento o al responsabile della protezione dati (R.P.D / D.P.O.) secondo le modalità previste dall'art. 12 commi 3 e 4 di cui al Reg. EU 2016/679.
8. Nel caso l'interessato venga autorizzato alla visione delle immagini per l'esercizio dei diritti di cui al comma 1 del presente articolo, lo stesso potrà visionare le immagini secondo le modalità previste dall'art. 13 del presente regolamento ed in ogni caso sotto la supervisione di personale autorizzato ai sensi di tale articolo. La supervisione da parte di tali soggetti non è richiesta laddove l'interessato

faccia accesso alle immagini accompagnato da personale di forza di polizia o esibendo un provvedimento dell'autorità giudiziaria che motivi l'accesso dell'interessato alle immagini.

9. L'accesso sarà in ogni caso registrato ai sensi dell'art. 19, comma 8 del presente regolamento.
10. 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. 20 Sicurezza Dei Dati

1. I dati sono protetti da 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. Vanno comunque assicurate misure adeguate ai sensi dell'articolo 32 GDPR.
3. Il Designato provvede a predisporre e verificare il corretto funzionamento dei sistemi di backup centralizzati, adottando idonee procedure per la custodia delle copie di sicurezza dei dati e delle applicazioni, nonché per il ripristino della disponibilità dei dati e dei sistemi, verificando periodicamente la leggibilità e l'integrità dei dati

- contenuti nelle copie di backup, effettuandone il ripristino.
 4. Il Designato provvede ad adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici, atti a mantenere la completezza e l'inalterabilità dei log. Tali registrazioni dovranno avere e mantenere le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità.
 5. Il Designato deve assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in azienda.
 6. Il titolare deve assicurarsi che siano designate per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.
 7. Il Designato deve individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).
 8. La trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie WiFi, WiMax, Gprs).
 9. Qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale.
 10. I dati personali oggetto di trattamento sono custoditi in un hard disk esterno a stato solido con crittografia integrata da algoritmo di crittografia sicuro, dotato di protezione password, rendendo i dati memorizzati più sicuri, custodito presso il Comando di Polizia Locale, in un luogo chiuso al pubblico, e accessibile esclusivamente per le persone autorizzate al trattamento dei dati. Non possono accedervi altre persone se non sono accompagnate da soggetti autorizzati.
- Art. 21 Modalità di**
autenticazione e credenziali
1. Il monitor nel quale potranno essere visualizzate le immagini registrate è collocato in modo tale da non permettere la visione delle immagini,

- neanche occasionalmente, a persone estranee non autorizzate.
2. L'accesso ai dispositivi e relativi dati di videosorveglianza di cui al presente disciplinare, avviene esclusivamente da postazioni dedicate situate all'interno dei locali delle strutture comunali in cui sono ubicati i monitor di controllo. L'accesso ai dati può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate dal responsabile della gestione tecnica degli impianti di videosorveglianza.
 3. L'accesso alle immagini da parte del Designato e delle persone autorizzate al trattamento dei dati si limita alle attività oggetto della sorveglianza; eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione.
 4. Nel caso le immagini siano conservate, i relativi supporti vengono custoditi, per l'intera durata della conservazione, in un armadio o simile struttura dotato di serratura, apribile solo dal designato ed ai responsabili della gestione tecnica dei dispositivi di videosorveglianza.
 5. Un file di log, generato automaticamente dal sistema informatico, consente di registrare gli accessi logici effettuati dai singoli operatori, le operazioni dagli stessi compiute sulle immagini registrate ed i relativi riferimenti temporali. Tale file non è soggetto a cancellazione.
 6. In caso di accesso di persone non autorizzate alla visione delle immagini dell'impianto di videosorveglianza, gli incaricati dovranno prendere tutte quelle misure ritenute necessarie ivi compreso l'oscuramento, momentaneo del monitor di controllo ovvero altre misure impartite dal titolare del trattamento dati.
 7. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure tecnologiche più avanzate; le operazioni di cancellazione devono essere effettuate esclusivamente sul luogo di lavoro.
 8. Nel caso il supporto debba essere sostituito per eccessiva usura, sarà distrutto in modo da renderlo inutilizzabile, in modo che non possano essere recuperati i dati in esso presenti.
 9. L'accesso alle immagini ed ai dati personali è consentito:
 - ✓ al Designato ed alle persone autorizzate dello specifico trattamento di cui all'art. 17 comma 1;
 - ✓ ai preposti alle indagini dell'Autorità Giudiziaria o di Polizia;
 - ✓ all'Amministratore di Sistema del Comune di Monopoli e alla ditta fornitrice delle apparecchiature nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione.
 10. Tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposito "registro degli accessi" (cartaceo od informatico), conservato

presso l'Ufficio Segreteria Comando, nel quale sono riportati ad opera delle persone autorizzate:

- ✓ la data e l'ora dell'accesso;
- ✓ l'identificazione del terzo autorizzato;
- ✓ i dati per i quali si è svolto l'accesso;
- ✓ gli estremi e la motivazione dell'autorizzazione all'accesso;
- ✓ le eventuali osservazioni della persona autorizzata;
- ✓ la sottoscrizione del medesimo.

Art. 22 Diritti dell'interessato

1. In qualunque momento, relativamente ai dati degli interessati, mediante comunicazione da inviarsi all'indirizzo e-mail urpmonopoli@comune.monopoli.ba.it, o mediante comunicazione scritta da inviare al Sindaco del Comune di Monopoli oppure all'attenzione del Dirigente dell'Area Organizzativa competente, gli stessi hanno il diritto di ottenere l'accesso alle proprie informazioni (art.15 del GDPR), la loro rettifica o integrazione (art.16 del GDPR), la loro cancellazione, la limitazione del trattamento (art.18 del GDPR) il diritto alla portabilità dei Suoi dati (art.20), il diritto di opporsi al trattamento dei propri dati per motivi particolari (art. 21 del GDPR) ai sensi del Regolamento (UE) n. 2016/679.
2. Il diritto di ottenere una copia di cui al comma 1, non deve ledere i diritti e le libertà altrui.

3. Il titolare del trattamento fornisce, a richiesta dell'interessato, una copia dei dati personali oggetto di trattamento.
4. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi comprensivi dei costi del personale, secondo le modalità previste dalla normativa vigente.
5. Poiché i dati acquisiti vengono trattati esclusivamente per le finalità di Polizia Giudiziaria nonché di protezione di persone e/o cose, non è previsto il diritto di limitazione ed opposizione per tali finalità, inoltre le istanze di cancellazione e opposizione potranno essere accolte solo qualora non siano più sussistenti le finalità di interesse pubblico.

Art. 23 Comunicazione dei dati

1. La comunicazione dei dati personali da parte del Comune di Monopoli a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria ed esclusivamente per lo svolgimento delle funzioni istituzionali.
2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, 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 e che operano sotto la loro diretta autorità.

3. È in ogni caso fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del D.Lgs. 30/6/2003, n. 196, così come modificato dal D.lgs. 101/2018, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.
4. Laddove sussistano i presupposti di cui all'art. 4 della Legge n. 300/1970 il sistema di videosorveglianza disciplinato dal presente regolamento viene posto in essere previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro.

Art. 24 Accertamento di illeciti e indagini delle autorità giudiziarie e/o di polizia

1. Ove dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale la persona autorizzata al

trattamento di videosorveglianza provvederà a darne immediata comunicazione agli organi competenti.

2. In tali casi, anche in deroga alle prescrizioni di cui ai precedenti articoli 18, 19, 34 e 35 del presente Regolamento, l'autorizzato al trattamento procederà agli ingrandimenti delle immagini strettamente necessari e non eccedenti allo specifico scopo perseguito ed alla registrazione delle stesse immagini su supporti magnetici.
3. Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli operatori di polizia e l'Autorità Giudiziaria.
4. Gli apparati potranno essere utilizzati anche in relazione ad indagini dell'Autorità Giudiziaria e degli operatori di Polizia Giudiziaria.
5. I trattamenti di dati personali dal Corpo di Polizia Locale effettuati per le finalità di polizia, quando direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati NON sono disciplinati dal presente regolamento ma sono disciplinati dal Decreto del Presidente della Repubblica del 15 gennaio 2018, n. 15 "*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. (GU Serie Generale n.61 del 14-03-2018) e dal D.lgs. del 18 maggio 2018, n. 51, recante: "Attuazione della direttiva (UE) 2016/680 del Parlamento e del consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2018/977 GAI del Consiglio".

Art. 25 Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti, ceduti o conservati secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e dell'art. 2 del D.lgs. 51/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Art. 26 Limiti alla utilizzabilità di dati personali

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati ai sensi dell'art. 2 decies del D.lgs. n. 196/03, salvo quanto previsto dall'art. 160 bis dello stesso decreto.

Art. 27 Danni cagionati per effetto del trattamento di dati personali

1. I danni cagionati ad altri per effetto del trattamento di dati personali comportano eventuale risarcimento ai sensi dell'art. 2050 del Codice Civile.

Art. 28 Destinatari dei dati personali trattati

6. I dati degli interessati per le finalità di cui al Punto 6 della presente informativa potranno essere comunicati a:
 - ✓ soggetti autorizzati dal Titolare del trattamento per l'espletamento delle attività necessarie alla gestione degli eventuali fatti che conseguano ai fatti illeciti verificatisi;
 - ✓ Autorità di pubblica sicurezza e all'Autorità giudiziaria, a seguito di richiesta scritta e/o per esigenze di difesa del Titolare;

- ✓ Autorità competenti in relazione ai procedimenti cui possono dar luogo gli eventi registrati;
- ✓ terzi in evasione di eventuali compatibili istanze di accesso presentate ai sensi di legge;
- ✓ agli interessati che intendono esercitare i propri diritti, sussistendone i presupposti.

7. Le videoregistrazioni in nessun caso saranno oggetto di diffusione.

8. Tutti i destinatari dei dati sono comunque vincolati al rispetto della riservatezza.

Art. 29 Violazione Dei Dati Personali

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune di Monopoli.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo

essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:

- ✓ danni fisici, materiali o immateriali alle persone fisiche;
- ✓ perdita del controllo dei dati personali;
- ✓ limitazione dei diritti, discriminazione;
- ✓ furto o usurpazione d'identità;
- ✓ perdite finanziarie, danno economico o sociale.
- ✓ decifratura non autorizzata della pseudonimizzazione;
- ✓ pregiudizio alla reputazione;
- ✓ perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- ✓ coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;

- ✓ riguardare categorie particolari di dati personali;
 - ✓ comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
 - ✓ comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
 - ✓ impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.

Art. 30 Tutela Amministrativa e Giurisdizionale

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 140 bis e seguenti del decreto legislativo 30 giugno 2003, n. 196, così come modificato dal D.lgs. 101/2018.
2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il designato al trattamento dei dati, così come individuato dal precedente art. 9.

Art. 31 Tutela dei dati personali

1. Il Titolare garantisce, nelle forme ritenute più idonee, che il trattamento dei dati personali in suo possesso si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, ai sensi delle vigenti disposizioni in materia.

Art. 32 Pubblicità del disciplinare

1. Copia del presente disciplinare, a norma dell'art. 22 della legge 7 agosto 1990, n. 241, è tenuta a disposizione del pubblico perché ne possa prendere visione in qualsiasi momento.
2. Il presente disciplinare verrà pubblicato all'Albo pretorio e sul sito internet istituzionale dell'Ente, nella sezione "amministrazione trasparente", ai sensi

della vigente normativa in tema di pubblicazione degli atti amministrativi

3. Per tutto quanto non subordinato dal presente disciplinare si fa rinvio alle disposizioni legislative e regolamentari in vigore in materia di protezione e trattamento dei dati personali nell'ambito della video sorveglianza.

Art. 33 Sopravvenienza di nuove disposizioni normative

1. Le disposizioni del presente disciplinare si intendono modificate per effetto di sopravvenute norme vincolanti statali, regionali o comunitarie.
2. In tali casi si applica la normativa sovraordinata. L'Ente potrà in ogni caso provvedere ad aggiornare il presente disciplinare per renderlo maggiormente conforme alle eventuali disposizioni normative intervenute.

Art. 34 Entrata in vigore e successive modifiche del regolamento

1. Il presente regolamento entra in vigore il giorno successivo alla pubblicazione all'Albo Pretorio della delibera di approvazione.
2. I contenuti del presente regolamento sono aggiornati nei casi di aggiornamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della protezione dei dati personali o atti

regolamentari generali del Consiglio dell'Unione dovranno essere immediatamente recepiti.

3. Laddove ne sussistano i presupposti di legge il presente regolamento è trasmesso al Garante per la protezione dei dati personali a Roma, sia a seguito della sua approvazione, sia a seguito dell'approvazione di suoi successivi ed eventuali aggiornamenti.