

# REGOLAMENTO SULLA VIDEOSORVEGLIANZA

## CAPO I

### PRINCIPI GENERALI

#### **Art. 1 – Premessa**

Il presente regolamento definisce la funzionalità del sistema di telecamere fisse e mobili di videosorveglianza e disciplina il trattamento e la protezione dei dati personali raccolti mediante i suddetti impianti.

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

Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune di barletta (BT), venga svolto nel completo rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza ed all'identità personale.

#### **Art. 2 - Norme di riferimento e principi generali**

Il presente regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto di videosorveglianza cittadina, attivato all'interno del territorio di competenza.

Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disciplinato dalla normativa vigente, in materia di videosorveglianza e trattamento dei dati personali:

- 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”.
- 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”.
- Decreto Legislativo n. 51 del 18 maggio 2018 - Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.
- Decreto Legislativo n. 196 del 30 giugno 2003 - Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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.

- Decreto Legislativo n. 101 del 10 agosto 2018 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- Decreto Legge 20 febbraio 2017, n.14 - art.5, convertito con modificazioni dalla legge 18 aprile 2017, n.48 (Patto per l'attuazione della sicurezza urbana).
- 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".
- 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).
- Decreto del Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008).
- Linee Guida n. 3/2019 dell'European Data Protection Board sulla videosorveglianza.
- FAQ sulla videosorveglianza pubblicate dal Garante per la Protezione dei Dati Personali del 2020.
- Linee Guida ANCI sulla videosorveglianza del 2010.
- Linee Guida ANCI per l'attuazione della sicurezza urbana del 2018.

La Videosorveglianza in ambito Comunale si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5 del GDPR, di seguito riportati:

**Principio di liceità** – Il trattamento di dati personali da parte di soggetti pubblici è lecito allorché si riveli necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ossequio al disposto di cui all'art. 6, Paragrafo 1, lett. e), GDPR. La videosorveglianza pertanto è consentita senza necessità di consenso da parte degli interessati.

**Principio di necessità** – In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. "minimizzazione dei dati") di cui all'art. 5, Paragrafo 1, lett. c), GDPR, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, l'utilizzo di dati anonimi o di opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi o ridondanze nei sistemi di videosorveglianza.

**Principio di proporzionalità** – La raccolta e l'uso delle immagini devono essere proporzionati rispetto 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, deve essere 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 come insufficienti o come inattuabili. Se la installazione di detti impianti 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 deve essere valutata in ogni fase o modalità del trattamento. Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare la visuale sull'area effettivamente da proteggere.

**Principio di finalità** – Ai sensi dell'art. 5, Paragrafo 1, lett. b), GDPR, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. È consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana che il D. M Interno 05/08/2008 definisce come il “bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale.”

#### **Art. 4 – Definizioni**

Ai fini del presente Regolamento si intende:

- per «**dato personale**», qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- per «**trattamento**», qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- per “**banca dati**”, il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;
- per «**titolare del trattamento**», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- per «**responsabile del trattamento**» (di seguito “Responsabile”), la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del Titolare (art. 4 del GDPR).

- per «**responsabile della protezione dei dati (DPO o RPD)**», il soggetto (interno o esterno) a cui il Titolare, o il Responsabile, si affida per garantire la conformità dell'organizzazione ai requisiti stabiliti dal Regolamento.
- per «**soggetto designato**», la nuova «figura» introdotta da decreto legislativo 101/2018 che prevede il potere del Titolare e/o del Responsabile, di delegare compiti e funzioni a persone fisiche che operano sotto la loro autorità e che, a tal fine, dovranno essere espressamente designati per «specifici compiti e funzioni» connessi al trattamento dei dati;
- per «**autorizzato o incaricato al trattamento**», la persona fisica che agendo sotto l'autorità del Titolare, ha accesso ai dati personali e compie materialmente le operazioni di trattamento;
- per «**interessato**», la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
- per «**destinatario**», il soggetto cui vengono comunicati i dati personali;
- per «**terzo**», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare;
- per «**pseudonimizzazione**», il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- per «**profilazione**», qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- per «**violazione dei dati personali**», la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- per «**comunicazione**», il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per «**diffusione**», il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per «**dato anonimo**», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

## **Art. 5 – Finalità istituzionali dei sistemi di videosorveglianza**

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

- D.Lgs. 31 marzo 1998, n. 112; D.Lgs. 18 agosto 2000, n. 267 (TUEL);
- L. 24 luglio 2008, n. 125, recante misure urgenti in materia di sicurezza pubblica;
- L. 23 aprile 2009, n. 38;
- D. Lgs. 15 maggio 2018, n. 51;
- D.P.R. 24 luglio 1977, n.616;

- Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana;
- 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.

In particolare, il sistema attivato dall'Amministrazione Comunale è finalizzato alla Tutela del Patrimonio Pubblico, dei beni Pubblici alla Sicurezza del Territorio, Controllare situazioni di degrado conseguenti all'abbandono di rifiuti e ad accertare l'utilizzo di aree impiegate come discariche abusive di rifiuti pericolosi e non pericolosi;

L'attività di videosorveglianza deve raccogliere unicamente 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 risultino indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.

La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi.

L'uso dei dati personali nell'ambito definito dal presente Regolamento non necessita del consenso degli interessati in quanto viene effettuato per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri e allo svolgimento di funzioni istituzionali di cui è investito l'Ente Comune di Barletta (BT).

#### **Art. 6 – Caratteristiche tecniche del sistema.**

Il trattamento dei dati personali è effettuato attraverso l'attivazione di un sistema di Videosorveglianza, le cui finalità istituzionali sono del tutto conformi a quelle, demandate all'Ente. Saranno trattati esclusivamente i dati personali rilevati mediante le riprese.

Le immagini possono essere esaminate da remoto, da persone a ciò debitamente formate ed autorizzate, ciò anche in orari di assenza dal servizio o in giorni festivi. Le riprese sono visibili anche in caso di scarsa illuminazione notturna.

Il Titolare procederà ad effettuare una valutazione sulla liceità e sulla proporzionalità del trattamento, stabilendo anche se sia necessaria o meno una valutazione d'impatto (DPIA) ai sensi degli artt. 35 del GDPR e 23 del D. lgs. 51/2018 o negli altri casi indicati dal Garante.

#### **Art. 7 – Informativa**

Gli interessati devono essere informati che stanno per accedere in una zona videosorvegliata. A tal fine l'Ente utilizzerà lo stesso modello semplificato di informativa "minima", riportante il Titolare del trattamento e la finalità perseguita, come da fac-simile di cui al punto 4 del FAQ sulla videosorveglianza e di seguito richiamato:



LA REGISTRAZIONE È EFFETTUATA DA .....

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

.....

FINALITÀ DELLA VIDEOSORVEGLIANZA .....

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

L'informativa completa sul trattamento dei dati è disponibile:

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

L'informativa va collocata prima di entrare nella zona sorvegliata. L'informativa deve rinviare a un testo completo contenente tutti gli elementi di cui all'art. 13 del Regolamento, indicando come e dove trovarlo (ad es. sul sito Internet del titolare del trattamento o affisso in bacheche o locali dello stesso).

### **Art. 8 – Responsabile del trattamento**

Laddove ritenuto necessario il Titolare potrà avvalersi di un responsabile del trattamento ai sensi dell'art. 4, par. 1, n. 8 GDPR. Il Responsabile elaborerà i dati personali per conto del Titolare e dovrà 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. Il Responsabile sarà individuato tramite atto scritto che definirà il rapporto con il Titolare, specificando gli obblighi e i limiti del trattamento dei dati. Il Responsabile riceverà, da parte del Titolare, tutte le istruzioni in merito ai trattamenti autorizzati e che potranno essere effettuati per conto del Titolare e alle quali dovrà attenersi. Inoltre, il Responsabile del trattamento dovrà mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento, e ove previsto, dovrà tenere il registro dei trattamenti svolti (ex art. 30, paragrafo 2, GDPR).

### **Art. 9 – Autorizzati al trattamento**

Il Titolare o il Responsabile del trattamento, procedono ad individuare con proprio atto, le persone fisiche autorizzate al trattamento dei dati, all'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, alla visione delle registrazioni.

L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato.

In ogni caso, prima dell'utilizzo degli impianti, gli autorizzati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno

conformare la propria condotta al pieno rispetto del medesimo. Gli autorizzati procedono al trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

In particolare, gli autorizzati 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 Titolare 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 Titolare del trattamento dei dati a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

Tra i soggetti designati quali autorizzati verranno individuati, con l'atto di nomina, le persone cui è affidata la custodia e la conservazione delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti magnetici.

Verranno inoltre designati, laddove necessario e con atto scritto gli Amministratori di Sistema. Gli autorizzati al trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare.

L'utilizzo degli apparecchi di ripresa da parte degli Incaricati al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato.

Responsabili ed autorizzati svolgono attività di verifica e controllo circa i principi di cui all'art. 5 del GDPR, adottino le misure tecniche di sicurezza, di cui all'art. 32 del GDPR, a garantire il tempestivo ripristino della disponibilità dei dati, a comunicare al Garante entro 72 ore eventuali violazioni dei dati personali, ad istituire ed aggiornare il Registro delle attività di trattamento ex art. 30 del GDPR.

#### **Art. 10 - Modalità di Raccolta e di Trattamento dei Dati**

L'attività di videosorveglianza deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.

Le telecamere di cui al precedente comma 1, consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario. Il Titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto

attivato. Potranno anche essere inviati segnali video delle unità di ripresa all' Unità di ricezione detenuta dall'Organo di Controllo.

I dati personali oggetto di trattamento sono: - trattati in modo lecito e secondo correttezza; - raccolti e registrati per le finalità di cui all'art. 5 del presente Regolamento.

### **Art. 11 - Sicurezza dei dati**

La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione.

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

I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, assicurano:

- a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
- c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Ai sensi dell'art. 32, par. 2 del GDPR, nel valutare l'adeguato livello di sicurezza, l'Amministrazione terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ente.

A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:

- a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini. Tenendo conto dello stato dell'arte ed in base alle caratteristiche dei sistemi utilizzati, i soggetti designati quali autorizzati al trattamento, dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le operazioni di competenza;
- b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime immagini operazioni di cancellazione o di duplicazione;
- c) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 9, dovranno essere predisposte misure tecniche per la cancellazione, in forma

automatica, delle registrazioni, al rigoroso scadere del termine previsto dalla normativa, in relazione alle specifiche attività istituzionali;

d) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini; e) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;

Il Titolare del trattamento vigila sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvedono altresì ad istruire e formare gli incaricati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati.

### **Art. 12 – Accesso ai dati**

L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 5 del presente Regolamento.

L'accesso alle immagini è consentito esclusivamente:

- a) al Titolare del trattamento;
- b) alle Forze di Polizia, nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);
- c) al Responsabile del Trattamento laddove nominato ed a ciò autorizzato (ad esempio la Società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo);
- d) all'Amministratore di Sistema (preventivamente individuato quale autorizzato al trattamento dei dati);
- e) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta al successivo art. 12 ed in base alle disposizioni del GDPR e del D. lgs. 51/2018. L'accesso da parte dell'interessato sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovranno essere utilizzate, da parte del Titolare o da parte del Responsabile del trattamento, accorgimenti tecnici e/o tecniche di oscuramento dei dati identificativi delle ulteriori persone fisiche eventualmente presenti nel video diverse dall'interessato;
- f) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22-28 della L. 241/1990 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/1990, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

## **Art. 13 - Diritti dell'interessato**

In relazione al trattamento di dati personali che lo riguardano, all'interessato sono riconosciuti i seguenti diritti:

- richiedere maggiori informazioni in relazione ai contenuti della presente informativa
- Diritto di accesso ai dati personali (art. 15 GDPR e art. 11 D.Lgs. 51/2018);
- Diritto di rettifica dei dati personali senza ingiustificato ritardo (art. 16 GDPR e art. 12 c.1 D.Lgs. 51/2018);
- Diritto di cancellazione dei dati. La cancellazione non è consentita per i dati contenuti negli atti che devono obbligatoriamente essere conservati dal Titolare (diritto all'oblio, art. 17 GDPR e art. 12 c.2 D.Lgs. 51/2018);
- Diritto di limitazione del trattamento (art. 18 GDPR e art. 12 c.3 D.Lgs. 51/2018);
- Diritto alla portabilità dei dati (art. 20 GDPR);
- Diritto di opposizione (art. 21 GDPR);
- Diritto relativo al processo decisionale automatizzato, compresa la profilazione (art. 22 GDPR e art. 8 D.Lgs. 51/2018).
- Diritto di proporre reclamo al Garante per la protezione dei dati personali (art. 77 GDPR e art. 39 D.Lgs. 51/2018), utilizzando la modulistica presente al seguente indirizzo:  
<https://www.garanteprivacy.it/home/modulistica-e-servizi-online>

L'istanza per l'esercizio dei diritti dell'interessato è presentata al Titolare dei dati dell'Ente, ai sensi dell'art. 38, par. 4 del GDPR.

Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare: il luogo, la data e la fascia oraria della possibile ripresa; l'abbigliamento indossato al momento della possibile ripresa; gli eventuali accessori in uso al momento della possibile ripresa; l'eventuale presenza di accompagnatori al momento della possibile ripresa; l'eventuale attività svolta al momento della possibile ripresa; eventuali ulteriori elementi utili all'identificazione dell'interessato.

L'incaricato del trattamento accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano. Qualora, ai sensi dell'art. 15, par. 3 del GDPR, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, par. 4 del GDPR.

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.

Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

## **Art. 14 – Mezzi di ricorso, di tutela amministrativa e di tutela giurisdizionale**

Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, GDPR, dal D. Lgs n. 196/2003, come modificato dal D. Lgs. 101/2018 ed agli artt. 37-42 del D. Lgs. n. 51/2018.

#### **Art. 15 - Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali**

Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile del trattamento ai sensi delle disposizioni di cui all'art. 82 del GDPR e dell'art. 2043 c.c.

Il Titolare o il Responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, par. 2 del GDPR.

#### **Art. 16 - Pubblicità del Regolamento**

Copia del presente Regolamento sarà pubblicata all'Albo Pretorio del Comune di Barletta (BT) e potrà essere reperita sul sito istituzionale dell'Ente, nell'apposita sezione dedicata ai Regolamenti.

#### **Art. 17 – Entrata in vigore**

Il presente Regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite. Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.