COMUNE DI PADRIA

PROVINCIA SASSARI

REGOLAMENTO PER LA DISCIPLINA DELL'IMPIANTO DI VIDEOSORVEGLIANZA

(*Deliberazione del Consiglio Comunale n. 38 del 25/11/2022*

INDICE

1) Principi generali

1.1 Oggetto

Col presente regolamento si disciplina il trattamento dei dati personali realizzato attraverso gli impianti di videosorveglianza installati nel territorio urbano del Comune di Padria. Attività quali la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini rappresentano dei trattamenti di dati personali ogniqualvolta abbiano ad oggetto una qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Il Comune di Padria, in qualità di Amministrazione aderente al Progetto della Regione Autonoma della Sardegna "Reti per la Sicurezza del Cittadino e del Territorio - Reti di Sicurezza - Fase 2", con il quale, attraverso un sistema centralizzato, si monitorano, visionano e trasferiscono, in tempo reale, i flussi video provenienti dalle reti locali di videosorveglianza delle Amministrazioni Locali aderenti, ha predisposto il proprio impianto di videosorveglianza affinché lo stesso sia pienamente interoperabile con le specifiche del DVMS Regionale (Digital Video Management System della RAS - Sistema di Gestione Video Digitale della Regione Autonoma della Sardegna) e con le Forze dell'Ordine collegate al sistema DVMS di cui sopra, nel rispetto delle norme sul trattamento dei dati personali e secondo i protocolli di sicurezza e gli standard tecnologici previsti dalla normativa.

Il Comune di Padria, in qualità di titolare del trattamento, può trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi e soltanto per lo svolgimento delle proprie funzioni istituzionali.

Le prescrizioni del presente regolamento si fondano sui principi applicabili al trattamento di dati personali, quali quello di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza richiamati dall'art. 5 del Regolamento europeo 2016/679 (GDPR) e dal Codice della privacy (D. Lgs. 196/03, come modificato dal D. Lgs. 101/2018), nonché dall'art. 3 del D. Lgs. 51/2018.

1.2 Principi generali

Il Comune di Padria, in ossequio al principio di liceità, prevede che il trattamento di dati personali ottenuti a mezzo dei sistemi di videosorveglianza venga effettuato esclusivamente per lo svolgimento delle funzioni istituzionali e nel rispetto dei presupposti e dei limiti stabiliti dal Regolamento UE 2016/679 GDPR, dal Codice della privacy, dalla Direttiva UE 2016/680 (cd. "Direttiva Polizia") e dal D. Lgs. 51/2018, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti. Il principio di liceità, infatti, prevede il rispetto, oltre che della disciplina in materia di protezione di dati personali, anche delle altre eventuali disposizioni che riguardino, ad esempio, le norme in materia di interferenze illecite nella vita privata, di controllo a distanza dei lavoratori, di sicurezza negli stadi e negli impianti sportivi e di sicurezza nell'ambito del trasporto urbano.
In ossequio al principio di necessità, ogni attività di trattamento dei dati personali acquisiti mediante gli impianti di videosorveglianza non può eccedere la soglia necessaria al raggiungimento degli scopi prefissati nel rispetto delle funzioni istituzionali. La predisposizione degli impianti di videosorveglianza, in sostanza, non può rappresentare di per sé un'esigenza dell'amministrazione comunale, ma deve essere preordinata al soddisfacimento di bisogni specifici.

Nel rispetto del principio di limitazione della finalità, limitazione della conservazione e minimizzazione dei dati, si prevede che tutte le fasi dell'attività di videosorveglianza siano improntate ad un trattamento di dati personali pertinenti e non eccedenti rispetto alle finalità perseguite dal Comune di Padria nell'ambito dello svolgimento delle funzioni istituzionali. Tale principio influenza l'Amministrazione comunale sin dalla scelta delle funzionalità e delle caratteristiche delle telecamere da installare nell'ambito del territorio urbano e sin dal momento dell'individuazione del numero dei soggetti designati ed autorizzati al trattamento dei dati.

I principi di limitazione della finalità del trattamento, sopra richiamato, nonché quello di correttezza e trasparenza, prevedono che gli scopi del trattamento siano legittimi (il soggetto che esegue il trattamento deve essere legittimato al perseguimento delle finalità del trattamento), determinati ed espliciti (ossia predeterminati e comunicati, mediante idonea informativa, agli eventuali interessati al trattamento).

Per tutto quanto non disciplinato dal presente regolamento si rinvia alle disposizioni del Regolamento Europeo 2016/679 GDPR, del Codice della privacy (D.lgs. 196/2003, come novellato dl D.Lgs. 101/2018 e, da ultimo, dalle novità introdotte dal decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205 e dal decreto-legge 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178), del D.Lgs. 51/2018 attuativo della cd. "Direttiva Polizia" (Direttiva UE 2016/680), al provvedimento del Garante Privacy in materia di videosorveglianza del 8 aprile 2010 (il quale, ai sensi dell'art. 22 del D.lgs. 101/2018, continua ad applicarsi, salvo che nelle parti in cui risulti incompatibile con le disposizioni del GDPR o del D.lgs. 101/2018), nonché alle Linee guida dell'EDPB (*European Data Protection Board* o "Comitato Europeo per la Protezione dei Dati") n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video nella versione 2.0 adottate il 29 gennaio 2020.

1.3 Definizioni

Ai fini del presente regolamento si intende per:

a) **"dato personale"**, qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) **"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;

c) **"titolare**", 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. Ai fini del presente regolamento il

titolare del trattamento dei dati personali è il Comune di Padria, nella persona del Sindaco "pro tempore";

d) **"responsabile del trattamento"**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento ai sensi dell'art. 28 del GDPR;

e) **"designato"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo istruiti e autorizzati dal Titolare, nel rispetto delle disposizioni di cui agli artt. 29 e 32.4 GDPR ed art. 2-quaterdecies del Codice della privacy, al trattamento di dati personali;

f) **"autorizzato"**, la persona fisica istruita e autorizzata a compiere operazioni di trattamento dal titolare o dal soggetto designato dal titolare, nel rispetto delle disposizioni di cui agli artt. 29 e 32.4 GDPR ed art. 2-quaterdecies del Codice della privacy;

g) **"interessato"**, la persona fisica cui si riferiscono i dati personali;

h) **"comunicazione"**, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate (ai sensi dell'articolo 2-quaterdecies del Codice della privacy) al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

i) **"diffusione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

l) **"dato anonimo"**, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

m) **"misure tecniche e organizzative"**, il complesso delle misure tecniche e organizzative di cui all'art. 32 del GDPR.

1.4 Normativa di riferimento

Il presente regolamento tiene conto oltre che del "Codice in materia di protezione dei dati personali", ossia il D.Lgs. 196/2003 e s.m.i., anche delle norme di cui al Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (pubblicato nella Gazzetta ufficiale dell'Unione europea L.119 del 4 maggio 2016), che trova applicazione a decorrere dal 25 maggio 2018. Inoltre, per il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, si è tenuto conto della disciplina dettata dal D.Lgs. 51/2018, attuativo della cd. "Direttiva Polizia", ossia la Direttiva (UE) 2016/680.

Rilevante in materia è anche il "Provvedimento in materia di videosorveglianza" dell'Autorità Garante per la Protezione dei Dati Personali datato 8 aprile 2010, il quale prescrive ai titolari del

trattamento di dati personali effettuato tramite sistemi di videosorveglianza di adottare particolari misure e accorgimenti concernenti, tra gli altri, gli obblighi di: rendere l'informativa visibile anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno; sottoporre i trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali degli interessati alla valutazione d'impatto di cui al capo IV, sezione 3 del GDPR; adottare le misure di sicurezza a protezione dei dati registrati tramite impianti di videosorveglianza e adottare le misure necessarie per garantire il rispetto di quanto indicato a proposito di utilizzo condiviso dei sistemi di videosorveglianza. Tale ultimo provvedimento del Garante - lo si ribadisce - ai sensi dell'art. 22 del D.lgs. 101/2018, continua ad applicarsi, salvo che nelle parti in cui risulti incompatibile con le disposizioni del GDPR o del D.lgs. 101/2018. Inoltre, si è tenuto conto delle recenti novità introdotte dall'EDPB (*European Data Protection Board*, ossia il "Comitato Europeo per la Protezione dei Dati") con le Linee guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate il 29 gennaio 2020.

Rilevante, inoltre, è il contenuto del D.L. 23 maggio 2008, n. 92, recante "*Misure urgenti in materia di sicurezza pubblica*", che ha modificato l'art. 54 del D.lgs. 267/2000 in materia di attribuzioni del sindaco nelle funzioni di competenza statale, prevedendo che questi, previa comunicazione al prefetto anche ai fini della predisposizione degli strumenti ritenuti necessari alla loro attuazione, possa (quale ufficiale del Governo) adottare con atto motivato provvedimenti "*contingibili e urgenti nel rispetto dei principi generali dell'ordinamento, al fine di prevenire e di eliminare gravi pericoli che minacciano l'incolumità pubblica e la sicurezza urbana*". A delimitare i concetti di "incolumità pubblica" e "sicurezza urbana" è successivamente intervenuto il Decreto Min. Interno 5 agosto 2008 prevedendo che "*per incolumità pubblica si intende l'integrità fisica della popolazione e per sicurezza urbana un 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*". Nell'ambito di tale definizione - e con riferimento all'art. 54 del D.lgs. 267/2000 così come risultante a seguito dell'intervento della Corte costituzionale con sentenza n. 115/2011 - il sindaco interviene per prevenire e contrastare: "*a) situazioni urbane di degrado o di isolamento che favoriscono l'insorgere di fenomeni criminosi, quali lo spaccio di stupefacenti, lo sfruttamento della prostituzione, l'accattonaggio con impiego di minori e disabili e i fenomeni di violenza legati anche all'abuso di alcool; b) situazioni in cui si verificano comportamenti quali il danneggiamento al patrimonio pubblico e privato o che ne impediscono la fruibilità e determinano lo scadimento della qualità urbana; c) l'incuria, il degrado e l'occupazione abusiva di immobili tali da favorire le situazioni indicate ai punti precedenti; d) situazioni che costituiscono intralcio alla pubblica viabilità o che alterano il decoro urbano, in particolare quelle di abusivismo commerciale e di illecita occupazione del suolo pubblico; e) comportamenti che, come la prostituzione su strada o l'accattonaggio molesto, possono offendere la pubblica decenza anche per le modalità con cui si manifestano, ovvero turbano gravemente il libero utilizzo degli spazi pubblici o la fruizione cui sono destinati o che rendono difficoltoso o pericoloso l'accesso ad essi*".

Di assoluto rilievo, ancora, il D.L. 23 febbraio 2009, n. 11, recante "*Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*", nella parte in cui (art. 6, commi 7 e 8) prevede che "*per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico*" e che "*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*".

Nella redazione del presente regolamento, inoltre, si è tenuto conto delle informazioni contenute nelle "Linee guida per i Comuni in materia di videosorveglianza alla luce del provvedimento Garante privacy 8 aprile 2020" elaborate dall'ANCI; della Circolare del Ministero dell'Interno n. 558/SICPART/421.2/70, contenente la Direttiva sui sistemi di videosorveglianza in ambito comunale; della Circolare Min. Interno n. 558/A/421.2/70 del 8 febbraio 2005, avente ad oggetto "*Sistemi di videosorveglianza. Definizione di linee guida in materia*"; della Circolare Min. Interno n. 558/A/421.2/70/195960 del 6 agosto 2010, avente ad oggetto "*Sistemi di videosorveglianza*", nonché della Circolare Min. Interno del 11 settembre 2020 avente ad oggetto "*Decreto-legge 20 febbraio 2017, n. 14, recante "Disposizioni urgenti in materia di sicurezza delle città, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48. Patti per l'attuazione della sicurezza urbana e installazione di sistemi di videosorveglianza*".

Per quanto riguarda, inoltre, la interconnessione, a livello territoriale, delle sale operative della polizia locale con le sale operative delle forze di polizia e la regolamentazione dell'utilizzo in comune di sistemi di sicurezza tecnologica finalizzati al controllo delle aree e delle attività soggette a rischio, dovranno considerarsi le linee generali delle politiche pubbliche per la promozione della sicurezza integrata, adottate ai sensi dell'art. 2 del D.L. 20 febbraio 2017, n. 14, convertito con modifiche nella Legge 18 aprile 2017, n. 48, recante "*Disposizioni urgenti in materia di sicurezza delle città*".

Con riferimento, inoltre, ai trattamenti di dati conseguenti all'uso degli impianti di videosorveglianza comunale da altri soggetti, dovrà aversi riguardo al D.M. Interno 24 maggio 2017 avente ad oggetto i "*trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196*" ed, in particolare, l'allegata scheda n. 15.

Infine, da ultimo, si è tenuto delle novità introdotte dalla legge 205/2021 di conversione con modificazioni del D.L. 139/2021 (la quale non si applica ai trattamenti in presenza effettuati nell'ambito del D.Lgs. 51/2018), che ha introdotto una moratoria, ossia ha vietato l'installazione e l'uso di sistemi di riconoscimento facciale sino al 01 dicembre 2023, data ultima per l'adozione di uno specifico provvedimento legislativo in materia.

2) Finalità dei trattamenti e tipologie di telecamere

Il presente regolamento assicura che il trattamento dei dati personali acquisiti mediante gli impianti di videosorveglianza gestiti dal Comune di Padria si svolga nel pieno rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche.

I sistemi di videosorveglianza sono configurati in modo da ridurre al minimo (minimizzazione), rispetto alle finalità istituzionali perseguite, il trattamento dei dati personali, in modo da arrivare ad escluderne il trattamento laddove le finalità istituzionali possano essere soddisfatte mediante dati anonimi (anche mediante misure di anonimizzazione successive all'acquisizione dei dati) o mediante misure che consentano di risalire all'identità dell'interessato solo al verificarsi di particolari condizioni o specifiche necessità.

Le attività di controllo dei sistemi di videosorveglianza avvengono prevalentemente presso la centrale operativa della Polizia Municipale di Padria e ciò, in particolare, per quanto riguarda gli impianti di videosorveglianza relativi al monitoraggio del traffico e alla rilevazione delle infrazioni al codice della strada. In questi ambiti di operatività degli impianti di videosorveglianza, le comuni operazioni di gestione, visualizzazione, interconnessione, registrazione e controllo degli impianti di videosorveglianza avvengono presso la suddetta centrale operativa.

Presso la medesima sede si trova anche l'impianto centralizzato per la tutela della sicurezza urbana, basato su tecnologia IP che, tuttavia, consente - nel rispetto delle norme sul trattamento dei dati personali - anche l'accesso remoto, tramite personale espressamente autorizzato all'accesso, alla gestione e alle operazioni sui dati (in streaming o memorizzati dal sistema). Si prevede che tale sistema di videosorveglianza basato su tecnologia IP, attualmente utilizzato per finalità di sicurezza urbana, sia destinato a coprire le altre finalità di videosorveglianza descritte dal presente documento.

Altri impianti di videosorveglianza sono dislocati e adeguatamente segnalati all'interno o all'esterno di edifici comunali quali musei, istituti scolastici o sedi della cultura.

Dietro specifico provvedimento o accordo con l’Autorità Giudiziaria o con la Polizia Giudiziaria può fornirsi la possibilità a questi ultimi di eseguire operazioni quali l’accesso, la visualizzazione in diretta o in differita, l’accesso alle registrazioni audiovisive o alla stessa possibilità di eseguire le registrazioni in autonomia, anche mediante l’interconnessione - attraverso reti dedicate o reti pubbliche, previa cifratura delle connessioni al fine di evitare che terzi possano intercettare in tutto o in parte il flusso di dati - con la centrale operativa della Polizia Municipale di Padria.

L’implementazione, lo sviluppo e la gestione degli impianti di videosorveglianza da parte del Comune di Padria soddisfano differenti finalità, quali:

- attuazione di un sistema di sicurezza urbana integrata, ai sensi dell’art. 2 del D.L. 14/2017, convertito nella Legge 48/2017 e s.m.i.;

- tutela della sicurezza urbana e della sicurezza pubblica;

- monitoraggio del traffico e sistema di lettura targhe O.C.R.;

- tutela della sicurezza stradale;

- tutela degli operatori e del patrimonio comunale;

- tutela della protezione civile e della sanità pubblica;

- tutela ambientale e polizia amministrativa;

- tutela degli immobili di proprietà o in gestione dell’Amministrazione Comunale e prevenzione di eventuali atti di vandalismo o danneggiamento;

- lotta all’abusivismo edilizio;

- rilevazione e accertamento delle violazioni dei Regolamenti e ordinanze comunali;

- prevenzione degli istituti scolastici da atti di vandalismo;

- attuazione di atti amministrativi generali (art. 2-ter Codice Privacy novellato dalla Legge 205/2021).

- tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. Si precisa che quest'ultima finalità è soggetta alla speciale disciplina dettata dalla Direttiva 2016/680/UE e dal D.lgs. 51/2018;

- arresto in flagranza differito (Art. 10, comma 6 quater, D.L. 14/2017, convertito nella Legge 48/2017 e s.m.i.);

- finalità promozionali, turistiche o pubblicitarie.

Ai sensi di quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300, così come modificato dal D.lgs. 151/2015 e dal D.lgs. 185/2016, gli impianti di videosorveglianza non possono essere utilizzati, salvi i casi previsti dal medesimo articolo, per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

Gli impianti di videosorveglianza situati presso la Centrale operativa della Polizia Municipale sono limitati nelle funzionalità, anche attraverso un eventuale settaggio e oscuramento automatico delle riprese in modalità non modificabile dall'operatore autorizzato al trattamento, in modo da escludere ogni forma di ripresa, anche in mancanza di registrazione, di particolari non rilevanti e di spazi interni relativi a private abitazioni.

2.1 Sicurezza urbana e sicurezza pubblica

Il Comune di Padria gestisce gli impianti di videosorveglianza anche per finalità di sicurezza urbana. A tal proposito si richiama la definizione di sicurezza urbana quale "*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*" di cui al Decreto Min. Interno 5 agosto 2008.

Tutte le operazioni di videosorveglianza per finalità di sicurezza urbana e di prevenzione e repressione degli atti delittuosi, delle attività illecite e degli episodi di microcriminalità commessi sul territorio comunale, e quindi sostanzialmente orientate ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana", devono essere funzionali rispetto ai compiti affidati al Comune di Padria.

Le immagini, per tali finalità, potranno essere visionate e gestite:

- sulla base di querele/denunce di atti criminosi da parte dei cittadini, per il successivo inoltro delle eventuali fonti di prova all'autorità giudiziaria;

- sulla base di segnalazioni relative ad atti criminosi accertate direttamente dagli organi di polizia in servizio sul territorio cittadino;

• sulla base di atti criminosi che vengono rilevati direttamente dagli operatori di polizia nel visionare le immagini trasmesse in diretta dalle telecamere, nell'esercizio delle proprie funzioni;

• sulla base di richieste specifiche per indagini da parte dell'autorità giudiziaria;

• sulla base di ogni altra richiesta di specifici organi/autorità che siano espressamente autorizzati, secondo specifiche norme di legge.

A tal fine le immagini sono custodite nel rispetto delle misure tecniche e organizzative adeguate, di cui all'art. 32 del GDPR, anche al fine di impedire trattamenti non autorizzati (confidenzialità, integrità e disponibilità dei dati). I locali della centrale operativa della Polizia Municipale di Padria o le altre postazioni attraverso le quali accedere, da remoto, ai sistemi di videosorveglianza per finalità di sicurezza urbana, prevedono - per le medesime finalità di sicurezza - modalità di accesso tali da escludere qualsivoglia trattamento a soggetti non autorizzati espressamente grazie a sistemi di allarme, accesso ai locali previa digitazione di codici personali o badge personali nella disponibilità degli autorizzati.

Della estrapolazione di immagini o di registrazione di sequenze audio/video degli impianti di videosorveglianza è tenuta idonea documentazione. L'accesso ai server in cui sono custodite le registrazioni o i pannelli di controllo degli impianti di videosorveglianza sono condizionati ad un'autenticazione di cui il sistema deve tenere evidenza.

La registrazione delle immagini raccolte al fine di soddisfare le finalità di cui al presente articolo sono conservate, nel rispetto dell'art. 6, comma 8, del D.L. 11/2009, per un massimo di 7 giorni successivi all'acquisizione. Qualora eventuali esigenze particolari dovessero richiedere un tempo superiore di conservazione, il Comune di Padria dovrà preliminarmente eseguire una DPIA - Valutazione di impatto privacy.

Inoltre, il sistema di videosorveglianza è utilizzato anche per finalità di sicurezza pubblica, in tutte le ipotesi in cui il trattamento dei dati personali ottenuti in conseguenza delle attività di videosorveglianza avvenga per finalità di polizia, ovvero sia direttamente correlato all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria. In tal caso, la correlata attività di prevenzione e repressione dei reati, svolta ai sensi del codice di procedura penale, soggiace alla disciplina normativa di cui alla Direttiva (UE) 2016/680 ed al D.lgs. 51/2018, che ne disciplina il recepimento. In considerazione dell'applicazione della Direttiva 2016/680 viene meno, tra l'altro, l'obbligo di prestare idonea informativa per le singole telecamere degli impianti di videosorveglianza.

Si precisa che gli agenti in servizio del corpo della Polizia municipale di Padria, nell'ambito territoriale del Comune di appartenenza - fatte salve disposizioni di legge speciale - si considerano agenti di polizia giudiziaria ai sensi dell'art. 57 c.p.p.

2.2 Monitoraggio del traffico e sistema di lettura targhe O.C.R.

Il sistema di videosorveglianza è impiegato anche al fine di monitorare le condizioni e il flusso del traffico nell'ambito urbano, nonché per verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici. Il sistema di videosorveglianza, pertanto, nel rispetto del principio di necessità è configurato in modo da ridurre al minimo il trattamento di dati personali, ad esempio

riducendo la definizione delle immagini in modo tale da non rendere riconoscibili i volti delle persone o le targhe delle autovetture, ovvero limitando le funzioni di zoom delle telecamere brandeggiabili.

Inoltre, sono impiegate tecnologie di videoripresa dotate di sistema di lettura targhe che, mediante strumenti di riconoscimento ottico dei caratteri (cd. "O.C.R."), permettono di registrare il transito dei veicoli in un determinato tratto stradale rilevando i caratteri alfanumerici della targa, anche al fine di contrastare gli illeciti stradali, i reati predatori, nonché per fini statistici.

Le banche dati con cui le informazioni rilevate vengono comparate sono sia gli archivi nazionali (sistema informativo della Motorizzazione civile, CED veicoli rubati ecc.), ma anche quelle generate direttamente dall'organo di polizia che dispone dell'impianto di videosorveglianza, e la finalità perseguita è quella di accertare i transiti abusivi da parte di veicoli da ricercare (rubati o segnalati per altre esigenze di polizia), ovvero di veicoli non in regola con gli obblighi assicurativi o di revisione, oppure di veicoli appartenenti a classi ambientali inquinanti.

Per ciò che concerne i tempi di conservazione delle immagini, fermo restando lo svolgimento di una "DPIA – Valutazione d'impatto privacy", nel rispetto del principio di "accountability" (responsabilizzazione) il Comune di Padria - anche alla luce delle indicazioni della legge 205/2021 di conversione del D.L. 139/2021 - prevede la conservazione fino a tre mesi per i dati registrati mediante sistemi di lettura targhe e fino a sei mesi i filmati di interesse investigativo, memorizzati per specifiche ed oggettive esigenze di indagine.

2.3 Abbandono di rifiuti e vigilanza ambientale

Gli impianti di videosorveglianza possono essere utilizzati dal Comune di Padria - previa prestazione di idonea informativa riportante tale finalità - per il monitoraggio di ipotesi di utilizzo abusivo di aree come discariche di materiali e di sostanze pericolose e solo nei casi in cui non sia possibile o risulti inefficace il ricorso ad altri strumenti e sistemi di controllo.

Gli impianti di videosorveglianza possono altresì essere utilizzati dal Comune di Padria - previa prestazione di idonea informativa riportante tale finalità - per il monitoraggio del rispetto delle regole circa modalità, tipologia ed orario di deposito dei rifiuti la cui violazione sia sanzionata amministrativamente, nei casi in cui non sia possibile o risulti inefficace il ricorso ad altri strumenti e sistemi di controllo.

2.4 Telecamere modulari (fototrappole)

Potranno essere posizionate, su tutto il territorio comunale, delle telecamere modulari (fototrappole) con generazione di allarmi da remoto per il monitoraggio attivo.

Le telecamere modulari mobili dovranno essere utilizzate esclusivamente nei luoghi teatro di illeciti penali o amministrativi, e, in quest'ultimo caso, esclusivamente nelle ipotesi in cui non sia possibile o risulti inefficace il ricorso ad altri strumenti e sistemi.

Qualora non sussistano necessità di indagine previste dal D.lgs. 51/2018 che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree. In quest'ultimo caso, anche al fine di evitare il rischio di sottrazione/danneggiamento delle fototrappole, i cartelli con l'informativa privacy

verranno collocati non in maniera puntuale in prossimità delle stesse, ma ad esempio nei pressi degli accessi alle aree interessate, come le provenienze da strade pubbliche urbane o extraurbane, senza necessità di posizionare il segnale in corrispondenza del raggio di azione dei dispositivi.

Solo i soggetti appartenenti alla Polizia locale o eventuali "vigili ambientali" incardinati nell'organico comunale e dotati di tale specifica qualifica potranno avere accesso alle immagini di videosorveglianza delle fototrappole.

L'utilizzo delle fototrappole sarà preceduto da una "DPIA – Valutazione d'impatto privacy" e il titolare del trattamento si impegna ad adottare adeguate misure di sicurezza ai sensi dell'art. 32 GDPR anche al fine di evitare il furto dei dati contenuti nelle stesse (ad esempio, provvedendo alla cifratura delle schede di memoria).

2.5 Body cam e dash cam

Gli operatori di Polizia Locale possono utilizzare, per i servizi a maggior rischio operativo, delle "Body Cam" (telecamere sull'operatore) e delle "Dash Cam" (telecamere a bordo dei veicoli di servizio), in conformità alle indicazioni contenute nella nota 26 luglio 2016, prot. n. 49612 del Garante della Privacy, con la quale sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi (da ultimo, sull'esclusione del sistema di *facial recognition* e la durata della conservazione delle immagini, vedere la newsletter dell'Autorità Garante per la Protezione dei Dati personali n. 481 del 10 settembre 2021: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9698442). L'utilizzo di tali dispositivi rientra nell'ambito di applicazione del D.lgs. 51/2018.

Per l'utilizzo delle stesse, è necessario aver svolto preventivamente una "DPIA – Valutazione d'impatto privacy" e, qualora dall'utilizzo dei dispositivi in questione possa derivare il controllo a distanza dei lavoratori, l'impiego - conformemente all'art. 4, comma 1, della legge 300/1970 (cd. "Statuto dei lavoratori") - dovrà essere subordinato al previo accordo sindacale o, in subordine, all'autorizzazione dell'Ispettorato del lavoro.

Il Comando del Corpo curerà la predisposizione di uno specifico disciplinare tecnico/operativo interno, da somministrare agli operatori di Polizia Municipale che saranno dotati di microcamere, con specificazione dei casi in cui le microcamere devono essere attivate, dei soggetti eventualmente autorizzati a disporre l'attivazione (ad es. il capo-pattuglia), delle fasi propedeutiche all'impiego operativo, delle modalità di impiego operativo (pre-registrazione e avvio delle riprese) delle operazioni autorizzate nel caso di emergenza, della gestione delle registrazioni e di ogni altra misura organizzativa e tecnica necessaria alla corretta e legittima gestione di detti dispositivi.

Le videocamere e le schede di memoria di cui sono dotati i sistemi di cui ai commi precedenti dovranno essere dotate di un numero seriale da annotarsi in un registro recante il giorno, l'orario, i dati indicativi del servizio e la qualifica e nominativo del dipendente.

La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato.

Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, per i servizi a maggior rischio operativo. L'ordine di attivazione e di disattivazione del dispositivo deve essere

emesso dall'Ufficiale di Polizia Giudiziaria che impiega direttamente la pattuglia o, in mancanza, dalla Centrale Operativa.

Al termine del servizio gli operatori interessati, previa compilazione di un foglio di consegna, affideranno tutta la documentazione video realizzata all'Ufficiale responsabile, il quale provvederà alla sua consegna al Comando.

Nel caso di avvio delle riprese, gli operatori dovranno fornire un'informativa minima, ossia un avviso orale circa l'avvio delle riprese, meglio se registrato. Tale comunicazione, che dovrà essere breve, immediatamente comprensibile e neutra, servirà a rendere conforme il trattamento, oltre ad aumentare l'effetto deterrente del dispositivo.

2.6 Istituti scolastici

Il sistema di videosorveglianza attivo presso istituti scolastici, nel rispetto di quanto previsto dal paragrafo 4.3 del provvedimento del Garante Privacy in materia di videosorveglianza del 8 aprile 2010, dovrà garantire il diritto dello studente alla riservatezza, prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione.

In tale quadro, potrà risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti. E' vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola.

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

2.7 Coinvolgimento dei privati

Il Comune promuove, per quanto di propria competenza, il coinvolgimento dei privati per la realizzazione di singoli impianti di videosorveglianza, orientati comunque su aree o strade pubbliche o ad uso pubblico, nel rispetto dei principi di cui al presente regolamento, previa valutazione di idoneità dei siti e dei dispositivi, normalmente senza connessioni al sistema centrale e senza possibilità di accesso ai filmati, ma con connessioni preferibilmente "stand alone".

I privati interessati assumono su di sé ogni onere per acquistare le attrezzature e renderle operative in conformità alle caratteristiche tecniche dell'impianto pubblico, le mettono a disposizione dell'Ente a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa. Il Comune può assumere su di sè gli oneri per la manutenzione periodica e la responsabilità della gestione dei dati raccolti.

Nei casi sopraelencati, in accordo con il Comune e previa stipula di apposita convenzione, i soggetti privati che hanno ceduto i propri impianti di videosorveglianza all'Ente possono decidere, con oneri a proprio carico, di affidare il controllo in tempo reale delle immagini ad un istituto di vigilanza privato, con il compito di allertare ed interessare in tempo reale le forze di polizia in caso di situazioni anomale.

2.8 Utilizzo di S.A.P.R. (cd. “Droni”) per finalità di videosorveglianza

I Sistemi aeromobili a pilotaggio remoto (SAPR), comunemente noti come “droni” (ossia i velivoli privi di persone a bordo pilotati a distanza con un radiocomando) possono essere utilmente impiegati per integrare i trattamenti per finalità di videosorveglianza, quali:

- controllo delle emergenze e monitoraggio del territorio;
- rilevazione degli abusi edilizi ed urbanistici e contrasto degli illeciti ambientali;
- rilievo di incidenti stradali;
- operazioni di contrasto al commercio abusivo;
- attività di contrasto dello spaccio di stupefacenti;
- supporto alle attività di Protezione civile, ricerca e soccorso a persone;
- sorveglianza di eventi pubblici e manifestazioni.

Il Comune si impegna a rispettare la normativa vigente, ossia il codice della navigazione e le leggi speciali in materia, il Regolamento di esecuzione UE 2019/947 relativo a norme e procedure per l’esercizio di aeromobili senza equipaggio, il Regolamento UE 2018/1139, il Regolamento E.N.A.C. “UAS-IT” – Edizione 1 del 4 gennaio 2021, le FAQ dell’ENAC, le FAQ elaborate da EASA, oltre ai principi generali in tema di trattamento di dati personali.

Inoltre, l’Ente dovrà rispettare il decreto del Ministero dell’interno del 13 giugno 2022 (pubblicato in G.U. n. 192 del 18 agosto 2022), adottato di concerto con i Ministri della difesa e delle infrastrutture e mobilità sostenibili, attraverso il quale sono disciplinate le modalità di impiego dei droni da parte delle Forze di polizia (così come individuate dall’art. 16 della legge 01 aprile 1981, n. 121).

Qualora i droni vengano adoperati nell’ambito della ordinaria attività di videosorveglianza urbana o di accertamento amministrativo, questi dovranno rispettare il GDPR e il Codice privacy, in particolare il principio di “minimizzazione dei dati”.

Inoltre, fatta salva la necessaria “DPIA - Valutazione d’impatto privacy”, è redatto dal Titolare del trattamento un disciplinare operativo, che individui le modalità e gli ambiti di impiego, le procedure di raccolta e conservazione dei dati, nonché gli adempimenti e le misure di sicurezza che gli operatori individuati dovranno mettere in atto a tutela dei dati personali acquisiti nel corso dell’attività di volo.

2.9 Videoriprese per finalità promozionali, turistiche o pubblicitarie

Le telecamere installate al fine di soddisfare eventuali finalità promozionali-turistiche o pubblicitarie mediante l’acquisizione e la diffusione via Internet dei video o delle immagini relative del Comune Padria sono configurate in modo da rendere non identificabili, nemmeno indirettamente, le persone fisiche riprese.

3) Trattamento dei dati personali

3.1 Il Titolare del trattamento

Il Comune di Padria è il titolare del trattamento dei dati personali (artt. 4, par. 1, n. 7 e 24 GDPR), rappresentato dal Sindaco *pro tempore*, in qualità di legale rappresentante dell'Ente, acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento. A tal fine al Comune di Padria, anche unitamente ad altro titolare, compete ogni decisione in ordine alle finalità e modalità del trattamento, agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Il titolare del trattamento dei dati personali:

a) definisce le linee organizzative per l'applicazione della normativa di settore;

b) effettua la "DPIA - Valutazione d'impatto" e, ove necessario, la consultazione preventiva;

c) nomina i designati e gli autorizzati per la gestione tecnica degli impianti di videosorveglianza ed i responsabili (esterni) del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti 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 degli impianti di videosorveglianza;

e) vigila sulla puntuale osservanza delle disposizioni impartite;

f) comunica all'Autorità Garante per la Protezione dei Dati personali (e agli interessati) le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali.

3.1.1 Nomina dei soggetti designati e autorizzati al trattamento dei dati personali

Il Comune di Padria, nella sua qualità di Titolare del trattamento dei dati personali acquisiti a seguito delle attività di videosorveglianza disciplinate dal presente regolamento - fatti salvi i casi in cui trovi applicazione la disciplina speciale di cui alla Direttiva 2016/680/UE e al D.Lgs. 51/2018 - individua per iscritto, mediante specifico atto di nomina ai sensi degli artt. 29, 32.4 GDPR ed art. 2-quaterdecies D.Lgs. 196/2003, uno o più soggetti designati/autorizzati nell'ambito delle attività di videosorveglianza, individuati tra soggetti che per esperienza, capacità ed affidabilità forniscano idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. La designazione è fatta per iscritto, con indicazione analitica dei compiti affidatigli.

Più precisamente, designati al trattamento dei dati sono:

- il Comandante della Polizia Locale per le telecamere collegate alla centrale operativa;

- gli altri Dirigenti/Responsabili dei servizi competenti per le telecamere a tutela del patrimonio comunale o non collegate alla centrale operativa della Polizia Locale. Tali designati vengono puntualmente individuati con atto del Titolare - Sindaco, che può impartire direttive e fornire indicazioni per la gestione ottimale della videosorveglianza.

I designati individuano e nominano, con proprio provvedimento, gli autorizzati alla gestione dell'impianto nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio.

Le operazioni di trattamento di dati personali nell'ambito della videosorveglianza, possono essere effettuate esclusivamente da persone fisiche autorizzate al trattamento dal titolare o dal designato,

per iscritto, con atto di nomina riportante la individuazione puntuale e analitica dell'ambito del trattamento consentito. Gli autorizzati operano sotto la diretta autorità del titolare, attenendosi scrupolosamente alle istruzioni impartite.

La nomina degli autorizzati al trattamento deve essere effettuata per un numero delimitato di soggetti, specie quando il titolare si avvalga di collaboratori esterni.

Negli atti di nomina degli autorizzati al trattamento nell'ambito della videosorveglianza sono analiticamente indicate, tra le altre: la possibilità di accedere ai locali ove siano situate le postazioni di controllo della videosorveglianza; la eventuale possibilità di utilizzare gli impianti, di visionare le immagini, di orientare le telecamere brandeggiabili, di modificare lo zoom o la definizione dell'immagine, di copiare o stampare le immagini, di gestire le registrazioni, di accedere ai server di memorizzazione.

Nell'atto di nomina dell'autorizzato al trattamento vengono tutte le opportune istruzioni in tema di misure adeguate di sicurezza e si individuano gli specifici livelli di accesso consentiti in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore.

Nelle ipotesi in cui il Comune di Padria affidi la gestione o la manutenzione degli impianti di videosorveglianza a un soggetto esterno all'amministrazione comunale, quest'ultimo deve considerarsi responsabile (esterno) del trattamento dei dati personali e il relativo rapporto deve essere regolato da un contratto o altro atto negoziale conforme all'art. 28 del GDPR. Gli eventuali dipendenti del soggetto esterno nominato responsabile del trattamento dovranno essere puntualmente e specificamente autorizzati al trattamento dal responsabile, che avrà cura di disciplinare i trattamenti autorizzati nel rispetto dei principi generali dell'art. 5 del GDPR.

3.1.2 Contratti o altri atti negoziali con i Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR

Il Comune, qualora ricorra a Responsabili esterni per i trattamenti di videosorveglianza (es: società che si occupa della manutenzione dell'impianto, o l'Amministratore di sistema), dovrà prevedere, nei bandi e nei contratti, delle pattuizioni che disciplinino i seguenti profili:

a) Il Responsabile deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato;

b) Il Responsabile non può ricorrere ad altro responsabile senza autorizzazione scritta, specifica o generale;

c) Dovrà essere chiaramente individuata la durata del trattamento, la natura e la finalità, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare;

d) I dati devono essere trattati soltanto su istruzione documentata del Titolare;

e) Le persone fisiche autorizzate al trattamento di dati personali devono essere impegnate alla riservatezza o abbiano un obbligo legale di riservatezza;

f) Il Responsabile deve adottare misure tecniche e organizzative adeguate ai sensi dell'art. 32 del GDPR.

g) Il Responsabile deve assistere il Titolare ai fine di soddisfare le richieste di esercizio dei diritti da parte dell'interessato, nell'adempimento degli obblighi di sicurezza (art. 32), nella notificazione delle violazioni di dati personali (artt. 33-34), nella valutazione d'impatto sulla protezione dei dati (art. 35) e nella consultazione preventiva (art. 36);

h) Il Responsabile deve, a scelta del titolare, cancellare o restituire tutti i dati personali, una volta terminata la prestazione del servizio;

i) Il Responsabile deve mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi, e deve cooperare con le attività di controllo, verifica e ispezione.

3.2 Informativa di I e II livello

Fatti salvi i trattamenti le cui finalità comportino l'applicazione della Direttiva 2016/680/UE e del D.Lgs. 51/2018 (che rendono facoltativa la prestazione dell'informativa sul trattamento dei dati personali), il Comune di Padria fornisce agli interessati, che accedono o transitano in luoghi ove siano attivi sistemi di videosorveglianza, un'idonea informativa mediante il modello semplificato di informativa "minima" (originariamente allegato al provvedimento del Garante privacy in materia di videosorveglianza dell'8 aprile 2010, ed oggi modificato a seguito dell'entrata in vigore delle Linee Guida dell'EDPB n. 3/2019 adottate il 29 gennaio 2020 (vedi paragrafo 7), tanto che la stessa Autorità Garante ha recepito tali indicazioni e, nel dicembre 2020, ha messo a disposizione dei titolari del trattamento un nuovo fac-simile di cartello al seguente *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9496244).

L'informativa ha lo scopo di avvisare gli interessati che stanno per accedere in una zona videosorvegliata ed è collocata prima del raggio d'azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti. L'informativa ha un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno e ingloba un simbolo o una stilizzazione di esplicita ed immediata comprensione al fine di informare se le immagini sono solo visionate o anche registrate.

L'informativa "minima" (o di I livello) riporta l'indicazione del titolare del trattamento (Comune di Padria) e delle finalità del trattamento, i contatti del DPO (affinché lo stesso possa essere contattato dagli interessati per l'esercizio dei diritti o ulteriori richieste), il periodo di conservazione delle immagini, e reca al suo interno un collegamento (ipertestuale, Codice QR o altro) all'informativa completa ed estesa (o di II livello) pubblicata nel sito internet istituzionale del Comune.

L'informativa può non essere resa quando i dati personali siano trattati per il perseguimento delle finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati e nelle ipotesi previste dalla Direttiva 2016/680/UE e dal D.Lgs. 51/2018.

L'informativa è fornita in corrispondenza ed entro il raggio di azione di ogni telecamera.

Qualora il raggio di azione fosse più esteso in considerazione della presenza di più telecamere, l'informativa sarà resa prima del raggio d'azione complessivo delle telecamere, sempre che le finalità di trattamento delle immagini acquisite dalle diverse telecamere siano identiche (fatti salvi i casi in cui l'informativa sia facoltativa).

3.3 Misure di sicurezza

I dati raccolti mediante il sistema di videosorveglianza sono protetti con misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, al fine di minimizzare i rischi 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, anche in relazione alla trasmissione delle immagini (art. 32 del GDPR).

Sono adottate specifiche misure tecniche ed organizzative che consentono al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa.

In particolare le misure di sicurezza devono rispettare i seguenti principi:

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

- per i sistemi configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente valutata la possibilità, per i soggetti espressamente abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;

- per quanto riguarda il periodo di conservazione delle immagini, devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;

- nel caso di interventi derivanti da esigenze di manutenzione, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;

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

- la trasmissione tramite una rete pubblica di comunicazioni o tramite sistemi *wireless* di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza;

- ciascun sistema informativo ed il relativo programma informatico vengono conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del

trattamento possono essere realizzate impiegando solo dati anonimi (ad esempio, con riferimento alle finalità esclusive di monitoraggio del traffico).

3.4 Durata delle registrazioni e conservazione dei dati

La conservazione viene limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura degli uffici, ovvero nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria o ad un protocollo siglato nell'ambito del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica (di cui all'art. 20, L. 121/1981).

Nell'ipotesi in cui l'attività di videosorveglianza sia finalizzata anche alla tutela della sicurezza urbana, il termine massimo di durata della conservazione delle informazioni e delle immagini è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione.

Le speciali esigenze di ulteriore conservazione oltre il termine di sette giorni sono precedute, ove necessario, da una "DPIA - Valutazione d'impatto privacy". L'esigenza di una conservazione più lunga può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.

Inoltre, previa effettuazione di una DPIA e nel rispetto del principio di "accountability" (responsabilizzazione), per i dati registrati mediante sistemi di lettura targhe il Comune di Padria - anche alla luce delle indicazioni della legge 205/2021 di conversione del D.L. 139/2021 - prevede la conservazione fino a tre mesi e fino a sei mesi i filmati di interesse investigativo, memorizzati per specifiche ed oggettive esigenze di indagine.

Sono impiegate misure tecniche o organizzative al fine di operare l'integrale cancellazione, anche in modalità automatizzata mediante sovra-registrazione delle informazioni allo scadere del termine previsto. Il sistema di cancellazione deve rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di *expiring* dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

3.5 Sistemi integrati di videosorveglianza

Nell'ambito dei trattamenti mediante sistemi integrati di videosorveglianza tra il Comune di Padria ed altri soggetti pubblici - mediante gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento che utilizzano le medesime infrastrutture tecnologiche - i singoli titolari possono trattare le immagini nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa.

E' prevista la possibilità di attivare un collegamento dei sistemi di videosorveglianza comunali con le sale o le centrali operative degli organi di polizia. L'attivazione del predetto collegamento deve

essere reso noto agli interessati mediante l'informativa, salvo i casi di informativa facoltativa ai sensi del D.lgs 51/2018.

Tali modalità di trattamento richiedono l'adozione delle seguenti misure di sicurezza ulteriori: 1) adozione di sistemi idonei alla registrazione degli accessi logici degli autorizzati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei designati e degli autorizzati da parte del titolare, comunque non inferiore a sei mesi; 2) separazione logica dei trattamenti di dati personali effettuati dai diversi titolari in relazione alle competenze istituzionali di ciascuna amministrazione.

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

3.6 Collegamenti tra centrale di Polizia municipale e Forze dell'ordine

I collegamenti tra i sistemi di videosorveglianza del Comune di Padria e le centrali Forze di Polizia sono adottati anche in applicazione della Circolare Min. Interno n. 558/SICPART/421.2/70 (Direttiva sui sistemi di videosorveglianza in ambito comunale) e dei relativi allegati tecnici.

Per quanto riguarda, inoltre, la interconnessione, a livello territoriale, delle sale operative della polizia locale con le sale operative delle forze di polizia e la regolamentazione dell'utilizzo in comune di sistemi di sicurezza tecnologica finalizzati al controllo delle aree e delle attività soggette a rischio dovranno considerarsi le linee generali delle politiche pubbliche per la promozione della sicurezza integrata, adottate ai sensi dell'art. 2 del D.L. 20 febbraio 2017, n. 14, convertito con modifiche nella Legge 18 aprile 2017, n. 48, recante "*Disposizioni urgenti in materia di sicurezza delle città*".

Con riferimento, inoltre, ai trattamenti di dati conseguenti all'uso degli impianti di videosorveglianza comunale da altri soggetti dovrà aversi riguardo al D.M. Interno 24 maggio 2017 avente ad oggetto i "*trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196*" ed, in particolare, l'allegata scheda n. 15.

4) Diritti degli interessati

4.1 Diritto di accesso ed altri diritti

I soggetti a cui si riferiscono i dati personali possono esercitare in qualsiasi momento i diritti sanciti dagli artt. 15-22 GDPR, nonché dagli artt. 11-14 del D.Lgs. 51/2018. Qui di seguito sono riportati i diritti che l'interessato può esercitare con riguardo alla videosorveglianza:

• il diritto di chiedere al Titolare l'accesso ai dati personali ed alle informazioni relative agli stessi, la rettifica dei dati inesatti o l'integrazione di quelli incompleti, la cancellazione dei dati personali (al verificarsi di una delle condizioni indicate nell'art. 17, paragrafo 1 del GDPR e nel rispetto delle eccezioni previste nel paragrafo 3 dello stesso articolo, ad esempio se i dati sono trattati illecitamente), la limitazione del trattamento dei dati personali (al ricorrere di una delle ipotesi indicate nell'art. 18, paragrafo 1 del GDPR, ad esempio i dati sono trattati illecitamente). Con riferimento al D.Lgs. 51/2018, l'accesso ai dati personali è regolato dagli artt. 11 e 14, quello di rettifica dagli artt. 12 e 14, quello di limitazione dagli artt. 12 e 14, mentre quello di cancellazione dagli artt. 12 e 14.

• il diritto di opporsi in qualsiasi momento al trattamento dei dati personali, alle condizioni previste dall'art. 21 GDPR. Il diritto di opposizione non è previsto dal D.Lgs. 51/2018.

• il diritto di proporre reclamo a un'autorità di controllo (Autorità Garante per la protezione dei dati personali - www.garanteprivacy.it), e di rivolgersi all'Autorità giudiziaria ordinaria;

I suddetti diritti sono esercitabili entro i limiti indicati dall'art. 3.5 del Provvedimento videosorveglianza. In particolare, in riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

Nell'esercizio dei diritti, l'interessato potrà farsi assistere da persona di fiducia ovvero potrà conferire delega o procura a persone fisiche, enti, associazioni o organismi, affinché esercitino per suo conto i diritti sopraelencati.

I diritti di cui al presente articolo, riferiti a persone decedute, possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di tutela, ferme restando le limitazioni individuate dall'art. 2-terdecies D.Lgs.196/2003.

Tutti i succitati diritti potranno essere esercitati mediante richiesta da inoltrarsi al Titolare del trattamento, anche per il tramite del Responsabile della protezione dei dati. Il modulo per l'esercizio dei diritti è disponibile sul sito del Garante Privacy, all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924.

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi soltanto laddove la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

4.2 Diritto di accesso civico generalizzato, ai sensi dell'art. 5 D.Lgs. 33/2013

Le immagini registrate costituiscono "dati e documenti detenuti dalle pubbliche amministrazioni", ai sensi dell'art. 5 del D.Lgs. 33/2013, e su di esse può essere esercitato il diritto di accesso civico generalizzato, laddove l'istanza "identifichi i dati, le informazioni o i documenti richiesti".

Nel rispondere alle istanze di accesso civico generalizzato, il Comune dovrà valutare con attenzione se sussista una delle ipotesi di esclusione o eccezione previste dall'art. 5-bis del D.Lgs. 33/2013 e

dalle relative linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del D.lgs. 33/2013, con particolare riguardo alla sicurezza pubblica e all'ordine pubblico, alla conduzione di indagini sui reati e loro perseguimento e alla protezione dei dati personali, ovvero la domanda di accesso riguardi un numero manifestamente irragionevole di dati e documenti che imporrebbe un carico di lavoro tale da paralizzare, in modo molto sostanziale, il buon funzionamento dell'amministrazione.

4.3 Accesso ai filmati

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

Ogni richiesta deve essere specifica, formulata per iscritto, motivata ed indirizzata al designato del trattamento dei dati competente entro tre giorni dall'evento.

In linea generale, l'accesso alla copia delle immagini è consentita solo previa verifica della sussistenza di un interesse qualificato ai sensi della Legge 241/1990. Ogni richiesta verrà, comunque, gestita nel pieno rispetto della disciplina dell'accesso agli atti.

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

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

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

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

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

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

5) Verifica del rispetto dei principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, ai sensi dell'art. 25 GDPR e dell'art. 16 D.Lgs. 51/2018

Il Comune dovrà, sia per gli impianti di nuova adozione, sia per gli impianti esistenti, accertare il rispetto dei principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita.

In particolare, prima di procedere al trattamento, dovranno essere adottate:

a) misure tecniche e organizzative adeguate, volte a attuare i principi del GDPR e integrare nel trattamento le necessarie garanzie e tutelare i diritti degli interessati;

b) misure tecniche e organizzative adeguate, volte a garantire che siano trattati, per impostazione predefinita, soltanto i dati necessari per ogni specifica finalità, con particolare riguardo alla quantità dei dati raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità ai dati.

6) Valutazione d'impatto sulla protezione dei dati (cd. "DPIA" ex art. 35 del GDPR ed art. 23 D.Lgs. 51/2018) e Consultazione preventiva (art. 36 ed art. 24 D.Lgs. 51/2018)

La valutazione d'impatto sulla protezione dei dati personali (cd. "DPIA", qui la pagina informativa dell'Autorità Garante: https://www.garanteprivacy.it/regolamentoue/DPIA) è prevista quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, e deve essere effettuata dal titolare del trattamento prima di procedere al trattamento.

Il Titolare, nello svolgimento della valutazione, deve consultare il Responsabile della protezione dei dati (DPO), che dovrà sorvegliarne lo svolgimento e fornire il proprio parere obbligatorio.

In particolare, la valutazione è richiesta laddove si effettui la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione è altresì richiesta, come evidenziato dalle Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del GDPR, nell'ipotesi di utilizzo di un sistema di videosorveglianza per il controllo del traffico laddove si utilizzi un sistema intelligente di analisi delle immagini per l'individuazione dei veicoli e il riconoscimento automatico delle targhe.

La valutazione deve contenere almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati.

Se il trattamento è stato sottoposto a verifica preliminare da parte dell'Autorità Garante prima del maggio 2018 e prosegua con le stesse modalità oggetto di tale verifica, la valutazione non è necessaria, salvo che non siano emersi nuovi rischi.

La valutazione d'impatto non deve essere obbligatoriamente pubblicata, ma l'Amministrazione potrà valutare se pubblicarla per estratto.

Qualora il Comune non sia in grado di individuare misure sufficienti a ridurre il rischio a livelli accettabili, e dunque qualora il rischio residuale continui a permanere elevato, si dovrà attuare la Consultazione preventiva con l'Autorità Garante.

7) Responsabile della protezione dei dati ("DPO" ex art. 37 del GDPR)

Il Responsabile della protezione dei dati, designato ai sensi dell'art. 37 del GDPR, deve essere tempestivamente e adeguatamente coinvolto nelle questioni riguardanti i trattamenti per finalità di videosorveglianza.

In particolare, il DPO:

a) può essere contattato dagli interessati, anche con riguardo ai trattamenti per finalità di videosorveglianza;

b) deve svolgere attività di consulenza sui trattamenti, anche a favore dei dipendenti che effettuino il trattamento;

c) deve sorvegliare l'osservanza delle norme in tema di protezione di dati personali, nonché del presente regolamento, e deve verificare l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale designato/autorizzato;

d) deve fornire, se richiesto, un parere sulla valutazione d'impatto sulla protezione dei dati (cd. "DPIA") di cui all'art 35 del GDPR e sorvegliarne lo svolgimento;

e) deve cooperare con l'Autorità Garante e fungere da punto di contatto.

8) Registro delle attività del trattamento (art. 30 GDPR) e videosorveglianza

Il Comune, in sede di redazione e aggiornamento del Registro delle attività di trattamento di cui all'art. 30, par. 1, GDPR, cura che siano correttamente riportati e adeguatamente descritti i trattamenti effettuati per finalità di videosorveglianza, con particolare riguardo alle finalità del trattamento, alle categorie degli interessati, alle categorie di dati personali, ai termini previsti per la cancellazione e alle misure di sicurezza tecniche e organizzative adottate ai sensi dell'art. 32 GDPR.

Il Comune verifica che gli eventuali Responsabili nominati ai sensi dell'art. 28 del GDPR adottino a loro volta il Registro delle attività di trattamento, ai sensi dell'art. 30, par. 2, del GDPR.

9) Violazione dei dati personali (cd. "data breach")

9.1 Notifica di una violazione dei dati personali (cd. "data breach") all'Autorità Garante per la Protezione dei Dati Personali (art. 33 GDPR)

Il Comune, in caso di violazione dei dati personali, deve notificare la violazione all'Autorità Garante per la Protezione dei Dati Personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, mediante l'apposita procedura telematica resa disponibile, a partire dal 01 luglio 2021, al seguente link: https://servizi.gpdp.it/databreach/s/. Qualora la notifica non sia effettuata entro tale termine, essa deve indicare anche i motivi del ritardo.

La notifica non deve essere effettuata se è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica contiene quantomeno:

a) la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di record interessati;

b) la comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati;

c) la descrizione delle probabili conseguenze della violazione e delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e/o per attenuarne i possibili effetti negativi.

È possibile altresì procedere con la notifica "per fasi" ogniqualvolta non sia possibile corredare la notifica di tutta la documentazione utile (ad es. perché l'indagine sul "data breach" non si è ancora conclusa e non si dispone di tutti gli elementi atti a circostanziarlo). Si procederà allora con una prima notifica sommaria (cd. "notifica preliminare"), seguita poi da quelle più dettagliate (cd. "notifica integrativa").

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione ("self assessment") che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza (https://servizi.gpdp.it/databreach/s/self-assessment).

Inoltre, lo stesso Garante ha messo a disposizione un fac-simile del modello di notificazione, utile per capire quali sono i campi da compilare nella procedura telematica (https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni).

Il Titolare del trattamento si impegna ad adottare una "policy di gestione dei data breach", della quale verrà data la massima diffusione all'interno dell'Ente.

Maggiori dettagli sul tema, ivi comprese le Linee guida in materia di notifica delle violazioni di dati personali WP250 e le Linee guida dell'EDPB n. 1/2021 sugli esempi riguardanti la notifica di violazioni di dati personali sono rinvenibili nella pagina dedicata dell'Autorità Garante per la Protezione dei Dati personali.

Infine, indipendentemente dalla notificazione o comunicazione, il Comune deve documentare qualsiasi violazione dei dati personali (nel cd. "Registro delle violazioni"), specificando le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, e conservare la relativa documentazione.

9.2 Comunicazione di una violazione dei dati personali all'interessato (art. 34 GDPR)

Il Comune, in caso di violazione dei dati personali, suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, deve comunicare la violazione agli interessati, senza ritardo.

La comunicazione deve essere redatta in linguaggio semplice e chiaro, e deve contenere:

a) la descrizione della natura della violazione;

b) la comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati;

c) la descrizione delle probabili conseguenze della violazione e delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e/o per attenuarne i possibili effetti negativi.

La comunicazione non è dovuta qualora:

- si siano adottate misure tecniche e organizzative adeguate di protezione, applicate ai dati personali oggetto della violazione, con particolare riguardo alle misure destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

- vengano successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, il Comune procede a una comunicazione pubblica o a una misura simile, quale la pubblicazione sul sito istituzionale, gli annunci sulle pagine social, i comunicati stampa e la pubblicazione di annunci a pagamento per un termine congruo al fine di informare gli interessati con analoga efficacia.

10) Tutela amministrativa e giurisdizionale

La tutela amministrativa e giurisdizionale in tema di trattamento di dati personali mediante videosorveglianza è regolata dagli artt. 77 e ss. del GDPR, dagli artt. 140-bis e ss. del Codice della privacy (D.Lgs. 196/03), nonché dagli artt. 37 e seguenti della Direttiva Polizia.

In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4, 5 e 6 della Legge 241/1990, è il designato al trattamento dei dati personali.

Avverso i provvedimenti in tema di accesso ai sensi dell'art. 5 del D.Lgs. 33/2013 può essere proposto ricorso dinnanzi il Tribunale Amministrativo Regionale, ai sensi dell'art. 116 del Codice del processo amministrativo di cui al decreto legislativo 2 luglio 2010, n. 104.

11) Disposizioni finali

11.1 Modifiche al presente Regolamento

Il presente regolamento dovrà essere aggiornato laddove intervengano modifiche normative in tema di trattamento di dati personali, nuovi provvedimenti dell'Autorità Garante per la Protezione dei Dati personali, ovvero significative modifiche nelle modalità e/o finalità dei trattamenti.

11.2 Entrata in vigore del presente Regolamento

Il presente Regolamento entra in vigore decorsi quindici giorni dalla data di pubblicazione all'Albo Pretorio online, fatti salvi gli eventuali tempi tecnici che si rendessero necessari per l'organizzazione del servizio.

Eventuali e successive modifiche al presente Regolamento entreranno in vigore decorsi quindici giorni dalla data di pubblicazione all'Albo Pretorio online, da effettuarsi dopo che la relativa deliberazione di approvazione, ovvero determina dirigenziale, sia divenuta esecutiva.

Siffatto Regolamento, nonché le eventuali e successive modifiche, sono inseriti nella raccolta ufficiale dei Regolamenti Comunali.

11.3 Rinvio

Per quanto non previsto dal presente Regolamento, si rinvia alla normativa europea e nazionale in materia di trattamento e protezione dei dati personali nonché ai Provvedimenti dell'Autorità di controllo.

Il presente Regolamento sarà aggiornato a seguito delle modifiche della normativa e dei Provvedimenti di cui al succitato paragrafo 10.1.

11.4 Norme abrogate

Con l'entrata in vigore del presente Regolamento si devono considerare abrogate le disposizioni regolamentari con esso contrastanti.

11.5 Pubblicità del presente Regolamento

Il presente Regolamento è pubblicato nel sito istituzionale del Comune di Padria.