



**COMUNE DI PERUGIA
S.O.SICUREZZA**

**REGOLAMENTO DEL SISTEMA DI
VIDEOSORVEGLIANZA PER LA SICUREZZA E LA
DISCIPLINA DEL TRATTAMENTO DEI DATI
PERSONALI**

Approvato con deliberazione del Consiglio Comunale n.87 del 03.10.2022

Si attesta che il presente Regolamento è conforme al testo depositato presso la U.O. Segreteria Organi Istituzionali e Comunicazione.

Sommario

CAPO I - PRINCIPI GENERALI	3
Art. 1 Oggetto e norme di riferimento	3
Art. 2 Definizioni	3
Art. 3 Finalità	4
Art. 4 Trattamento dei dati personali	7
CAPO II - OBBLIGHI E ADEMPIMENTI PER I SOGGETTI GESTORI DEL SISTEMA	7
Art. 5 Titolare del trattamento	7
Art. 6 Designato	7
Art. 7 Autorizzati alla gestione dell'impianto di videosorveglianza	9
Art. 8 Soggetti terzi	10
CAPO III - MISURE DI SICUREZZA DELL'IMPIANTO DI VIDEOSORVEGLIANZA	10
Art. 9 Accesso al sistema di videosorveglianza	10
Art. 10 Diritti dell'interessato	11
Art. 11 Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale	12
Art. 12 Norme per la gestione del sistema - Misure di sicurezza	12
CAPO IV - TRATTAMENTO DEI DATI PERSONALI SICUREZZA E LIMITI ALLA UTILIZZABILITA' DEI DATI	14
Art. 13 Modalità di raccolta e requisiti dei dati personali	14
Art. 14 Informazioni rese al momento della raccolta	15
CAPO VI ALTRI TRATTAMENTI	15
Art. 15 impianto di videosorveglianza non pubblico	15
Art. 16 Sicurezza cittadina	16
Art. 17 Rilevamento infrazioni al CdS	17
CAPO VII DISPOSIZIONI FINALI	18
Art. 18 Modifiche regolamentari e ampliamento del sistema	18
Art. 19 Rinvii ed abrogazioni	18
Art. 20 Entrata in vigore e pubblicazione	18
FAC-SIMILE del modulo per istanza di accesso ai filmati da parte di privato	19
FAC-SIMILE del modulo per comunicazione dei dati	22
FAC-SIMILE del modulo consegna materiale	23
FAC-SIMILE Informativa ex art. 13 GDPR	25

CAPO I - PRINCIPI GENERALI

Art. 1 Oggetto e norme di riferimento

1. Il presente regolamento disciplina il funzionamento del sistema della videosorveglianza per la sicurezza cittadina, il trattamento e la protezione dei dati personali raccolti mediante il suddetto impianto attivato nel territorio del Comune di Perugia.

2. Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto da:

- Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008);
- Legge n. 38/2009 recante “misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori”;
- Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);
- Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito GDPR) relativo “alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”;
- D.P.R. n. 15 del 15/01/2018 recante “Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia”;
- D. Lgs. 18/05/2018 n. 51 “Attuazione della Direttiva UE 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”;
- D. Lgs. 10/08/2018 n.101 “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”;
- Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, Versione 2.0, Adottate il 29 gennaio 20203.

3. Vengono altresì osservati i principi dettati nelle circolari del Capo della Polizia nr. 558/A/421/471 del febbraio 2005 e nr. 558/A/421.2/70/195960 del 6 agosto 2010 e i principi della direttiva 2016/680 in materia di trattamento dati da parte delle autorità competenti ai fini di prevenzione indagine, accertamento e perseguimento di reati.

Art. 2 Definizioni

Ai fini del presente regolamento si intende:

- a) per “**banca dati**”, il complesso di dati personali raccolti nel server dedicato, ubicato presso sede idonea del Comune di Perugia ; tale insieme di dati consiste in riprese video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente soggetti e mezzi di trasporto che transitano nell'area interessata;
- b) per “**trattamento**”, l'insieme delle operazioni svolte con o senza l'ausilio dei mezzi elettronici o comunque automatizzati;
- c) per “**dato personale**”, qualunque informazione relativa a persona fisica, identificata o identificabile anche indirettamente, e rilevata con la visione o il processamento di immagini effettuati attraverso il sistema di videosorveglianza;

- d) per **“titolare”**, il Comune di Perugia competente a disporre per l’adozione e il funzionamento dell’impianto di videosorveglianza nonché a definirne le finalità, le modalità del trattamento dei dati personali e delle misure di sicurezza per l’utilizzo del predetto impianto;
- e) per **“designato”**, la persona fisica legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento dei dati personali raccolti dall’impianto con facoltà di individuare e nominare soggetti autorizzati o subdesignati;
- f) per **“subdesignato”**, la persona fisica individuata e nominata dal designato per lo svolgimento di specifiche funzioni legate al trattamento;
- g) per **“autorizzati”**, le persone fisiche autorizzate a compiere operazioni di trattamento dal designato o dal subdesignato;
- h) per **“interessato”**, la persona fisica, cui si riferiscono i dati personali raccolti per il tramite del sistema di videosorveglianza;
- i) per **“comunicazione”**, il dare conoscenza dei dati personali a uno o più soggetti determinati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- j) per **“diffusione”**, il dare conoscenza di dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- k) per **“dato anonimo”**, il dato che in origine o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- l) per **“dato pseudoanonimo”**, il dato trattato in modo da non poter essere più attribuito ad un interessato specifico senza l’utilizzo di informazioni aggiuntive conservate separatamente e protette da misure di sicurezza;
- m) per **“blocco”**, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
- n) per **“profilazione”**, qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzare tali dati personali per valutare una persona fisica;
- o) per **“violazione dei dati personali”**, la violazione di sicurezza che comporta accidentalmente o illecitamente la distruzione, la perdita, l’accesso e la divulgazione non autorizzata ai dati personali trattati;
- p) per **“legge”**, il decreto legislativo n. 196 del 30 giugno 2003 “Codice in materia di protezione dei dati personali” e il Regolamento Europeo 679 del 2016 e successive modifiche ed integrazioni;
- q) per **“garante”**, il garante per la protezione dei dati personali;
- r) per **“dash cam”**, contrazione di dashboard camera (telecamera da cruscotto), si intende un dispositivo elettronico per l’acquisizione di immagini, applicabile sul parabrezza o sullo specchietto retrovisore dei veicoli utilizzate al fine di registrare gli eventi che accadono all’esterno della vettura nella direzione in cui tale dispositivo è rivolto ovvero durante il periodo di sosta.
- s) per **“impianti attivi all’interno di aree private”** si intendono quelli che registrano esclusivamente immagini all’interno di abitazioni private e/o loro pertinenze esclusive.

Art. 3 Finalità

1. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l’attivazione dell’impianto di videosorveglianza nel territorio del Comune di Perugia, collegato alla Centrale Operativa della Polizia Locale, nonché a quella delle Forze di Polizia a competenza generale e al Centro Operativo Comunale di Protezione Civile (nel seguito COC) quando attivo, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all’identità personale. Garantisce, altresì, i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento. Il sistema informativo dei dati ed i programmi informatici dell’impianto di videosorveglianza sono configurati riducendo al minimo indispensabile per la finalità per cui sono ritenuti utili, la raccolta dei dati

personali e dei dati identificativi. Non si configura come trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante la raccolta di dati anonimi.

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

- o Legge 7 marzo 1986, n. 65, sull'ordinamento della Polizia Municipale;
- o D.P.R. 24 luglio 1977, n.616;
- o Legge 241/90 e s.m.i.;
- o Normativa in tema di privacy;
- o D.Lgs. 31 marzo 1998, n. 112;
- o D.Lgs. 18 agosto 2000, n. 267 – TUEL;
- o Legge 24 luglio 2008, n. 125 recante misure urgenti in materia di sicurezza pubblica;
- o Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana;
- o Legge 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale;
- o 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;
- o D. Lgs. n.51/2018.

3. Nella richiamata cornice normativa e all'interno del nuovo sistema di lotta alla criminalità che attribuisce ai Comuni un ruolo strategico nel perseguire finalità di tutela della sicurezza pubblica, l'impianto di videosorveglianza del Comune di Perugia è precipuamente rivolto a garantire la sicurezza urbana che, l'art. 1 del Decreto del Ministero dell'Interno del 5 agosto del 2008, testualmente definisce come il "bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."

4. La disponibilità di video in diretta o di registrazioni disponibili tempestivamente presso il Comune costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale sul territorio comunale, in stretto raccordo con le altre Forze dell'Ordine che operano sul territorio. L'archivio dei dati registrati e conservati per il tempo stabilito per legge costituisce, infatti, un patrimonio informativo per finalità di Polizia Giudiziaria, con eventuale informativa nei confronti dell'Autorità Giudiziaria competente a procedere in caso di rilevata commissione di reati.

5. In particolare, il sistema di videosorveglianza attivato dall'Amministrazione e realizzato attraverso le videocamere posizionate nei siti di cui all'elenco mantenuto costantemente aggiornato dal Comune di Perugia, condiviso on line con tutte le forze dell'ordine, è finalizzato a:

- a) incrementare la sicurezza urbana e la sicurezza pubblica nonché la percezione delle stesse rilevando situazioni di pericolo e consentendo l'intervento degli operatori;
- b) prevenire, accertare e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" già richiamato; le informazioni sono da subito a disposizione della maggior parte delle altre forze di Polizia competenti a procedere nei casi di commissione di reati o potranno essere condivise con qualsiasi altro soggetto titolato;
- c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale, gli edifici pubblici e prevenire eventuali atti di vandalismo o danneggiamento;
- d) controllare le aree considerate a maggiore rischio per la sicurezza, l'incolumità e l'ordine pubblico garantendo un pronto intervento;
- e) acquisire elementi probatori in fattispecie di violazioni amministrative e/o penali

- f) al monitoraggio del traffico per essere d'ausilio alle decisioni in materia di circolazione stradale;
- g) attivare uno strumento operativo di protezione civile sul territorio comunale;
- h) controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche per rifiuti di ogni genere;
- i) verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;
- j) individuare e sanzionare le violazioni al codice della strada (soltanto attraverso specifici apparecchi omologati dalla MCTC);
- k) tutela di edifici e manufatti di carattere monumentale ed istituzionale, quali la sede degli organi elettivi della città, il Palazzo di Giustizia, la Fontana Maggiore, la Cattedrale e altri beni culturali della città;
- l) controllo di aree caratterizzate dall'essere punto di concentrazione di eventi, manifestazioni che possono essere causa di disordini e di turbativa dell'ordine pubblico;
- m) tutela di coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un elevato grado di sicurezza nelle zone monitorate;
- n) supporto al COC, qualora la posizione delle telecamere sia utile nelle fasi di gestione dell'emergenza che ha determinato l'istituzione o l'insediamento del COC stesso.

6. Sono attivabili impianti di foto-sorveglianza e video-sorveglianza mobili, posizionabili in aree del territorio comunale individuate dal Comando Polizia Locale oppure montate su veicoli di servizio e utilizzabili per le finalità indicate nel precedente comma 5 lettere f) g) h) i) j) del presente regolamento.

7. Gli impianti di videosorveglianza in quanto tali (non omologati dalla MCTC a tale scopo) non possono essere utilizzati per l'irrogazione diretta di sanzioni per infrazioni al Codice della strada, ma esclusivamente per l'eventuale invio da parte delle Centrali Operative di personale con qualifica di organo di polizia stradale per le contestazioni ai sensi del Codice della strada.

8. L'utilizzo di dispositivi elettronici (es. autovelox, photo-red semaforici e simili) per la rilevazione di violazioni al Codice della strada, in considerazione della peculiarità dei fini istituzionali perseguiti, è assoggettato alla disciplina di cui al presente regolamento e specificatamente trattato dalla specifica normativa di settore.

9. Ai sensi dell'art. 4 Legge 20 maggio 1970 n. 300 (Statuto dei lavoratori) gli impianti di videosorveglianza non potranno essere utilizzati, per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

10. L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.

11. L'installazione e l'attivazione del sistema di videosorveglianza non deve essere sottoposta all'esame preventivo del Garante della privacy, essendo sufficiente che il trattamento dei dati personali, effettuato tramite tale tipologia di impianto per lo svolgimento dei propri compiti istituzionali, avvenga previa informativa alle persone che stanno per accedere nell'area videosorvegliata, utilizzando a tale fine il modello semplificato predisposto in fac-simile dall'Autorità e siano adottate idonee misure di sicurezza informatica e di gestione, definite nel presente regolamento.

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

13. La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi e finalità di cui al presente Regolamento.

Art. 4 Trattamento dei dati personali

1. Il trattamento dei dati personali è effettuato attraverso il funzionamento dell'impianto di videosorveglianza. Presso le Centrali Operative della Polizia Locale e della Questura di Perugia e delle altre Forze di Polizia sono collocate le postazioni per la visione in diretta delle immagini riprese dalle telecamere e per gli accessi al sistema di videosorveglianza indicati nell'art.8 del presente regolamento.
2. Le finalità istituzionali del suddetto impianto, come dettagliate nell'art.3, sono del tutto conformi alle funzioni istituzionali demandate al Comune di Perugia.
3. Le immagini vengono visionate presso il Comando della Polizia Municipale, il Corpo di Guardia, la Questura di Perugia e le altre Forze di Polizia ed il COC quando attivo. Le immagini vengono visionate attraverso monitor collocati in maniera tale da non essere visibili dal pubblico ed in locali non accessibili al pubblico. Quando i monitor sono attivi l'accesso all'area è riservato esclusivamente al personale autorizzato.
4. Ogni ulteriore comunicazione dei dati personali da parte del Comune di Perugia a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria e solo esclusivamente per lo svolgimento delle funzioni istituzionali. Ove non strettamente necessario, i dati saranno comunicati oscurando l'identità degli interessati.

CAPO II - OBBLIGHI E ADEMPIMENTI PER I SOGGETTI GESTORI DEL SISTEMA

Art. 5 Titolare del trattamento

1. Al Comune di Perugia, nella sua qualità di titolare del trattamento dei dati personali, compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.

Art. 6 Designato

1. Il Comandante della Polizia Locale è nominato con atto del Sindaco quale soggetto "designato" al trattamento dei dati personali ai sensi e per gli effetti dell'art.2 comma 1° lett. f) del presente regolamento.
2. Il Sindaco, autonomamente o attraverso l'Assessore alla Sicurezza, può visionare le immagini del sistema di videosorveglianza presso la Centrale Operativa o il Corpo di Guardia del Comando di Polizia Locale, quando sia necessario per assumere decisioni in merito alle proprie funzioni, così come stabilito dalla Legge, salvo che siano in corso di svolgimento attività d'indagine.
Le modalità di accesso saranno stabilite dal titolare, nel rispetto dei principi di cui all'art.5 GDPR, con particolare riguardo al principio di minimizzazione e di limitazione delle finalità.
3. La visione del materiale viene sospesa se c'è necessità di compiere atti di polizia giudiziaria.
4. Il soggetto designato è tenuto al coordinamento delle attività e al controllo del trattamento è altresì tenuto a conformare la propria azione al pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente Regolamento.
5. Il soggetto designato al coordinamento delle attività e al controllo procede al trattamento dei dati attenendosi alle istruzioni impartite dal Titolare il quale, anche

tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

6. Le competenze proprie del soggetto designato al coordinamento delle attività e al controllo del trattamento sono analiticamente disciplinate nell'atto amministrativo di nomina, con il quale il Titolare provvede alla sua individuazione. In particolare, il soggetto designato al coordinamento delle attività e al controllo del trattamento:

- individua e nomina con propri atti i soggetti autorizzati al trattamento impartendo loro le apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, GDPR;
- fa sì che detti incaricati siano opportunamente istruiti e formati da parte del funzionario designato del trattamento con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati illeciti, di perdita, distruzione o danno accidentale dei dati;
- provvede a rendere l'informativa "minima" agli interessati;
- verifica e controlla che il trattamento dei dati effettuato mediante sistema di videosorveglianza sia realizzato nel rispetto dei principi di cui all'art. 5 del GDPR e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente; garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;
- assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- adotta, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del GDPR;
- garantisce l'adozione di idonee misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico di tipo hardware o tecnico riguardante la disponibilità del sistema;
- assicura l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;
- garantisce che il DPO (Responsabile della Protezione dei Dati) designato dal Titolare del trattamento sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;
- è responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione, perdita o esfiltrazione dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- assicura che gli incaricati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le attività strettamente necessarie al perseguimento delle finalità istituzionali;
- garantisce la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale individuato quale incaricato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del DPO (Responsabile della Protezione dei dati), necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;
- vigila sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi;
- comunica senza ritardo al Titolare ed al DPO eventuali violazioni di dati personali di cui sia venuto a conoscenza.

7. È consentito il ricorso alla delega scritta di funzioni da parte del soggetto designato attraverso l'individuazione di soggetti sub-designati a specifiche funzioni, previa comunicazione al Sindaco.

8. Procede, previa comunicazione al Sindaco, all'individuazione ed alla nomina dei soggetti responsabili del trattamento ai sensi dell'art.28 GDPR

9. I designati ed i sub-designati devono rispettare pienamente quanto previsto, in tema di trattamento dei dati personali e delle misure di sicurezza, dalle leggi vigenti e dalle disposizioni previste dal presente regolamento.

10. Il soggetto designato custodisce le chiavi per l'accesso ai locali del server contenente le registrazioni, le chiavi di eventuali armadi o cassette per la conservazione di qualsiasi supporto informatico contenenti copie di dati.

Art. 7 Autorizzati alla gestione dell'impianto di videosorveglianza

1. Il soggetto designato al coordinamento delle attività e al controllo del trattamento dei dati procede 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 nonché all'acquisizione delle stesse. 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 anche attraverso una nomina legata alla funzione.

2. In ogni caso, prima dell'utilizzo degli impianti, i soggetti 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.

3. Gli autorizzati, individuati tra soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati, procedono al trattamento attenendosi alle istruzioni impartite dal soggetto designato al coordinamento delle attività e al controllo il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari. In particolare, gli autorizzati devono:

- per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, e avendo cura di non lasciare aperto il programma che consente il trattamento con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare accessi non autorizzati e di consentire sempre l'individuazione dell'autore di qualsiasi azione sui dati;
- 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 evitando anche che all'area in cui sono presenti i monitor accedano soggetti non autorizzati;
- evitare di creare banche dati nuove contenenti dati personali senza autorizzazione espressa del soggetto designato;
- conservare i dati rispettando le misure di sicurezza predisposte dall'Ente secondo le direttive AGID;
- fornire al designato del trattamento dei dati, al supervisore ed al DPO (Responsabile della Protezione dei dati), a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo;

- comunicare senza ritardo al proprio referente eventuali violazioni di dati personali di cui sia venuto a conoscenza;
 - utilizzare il brandeggio PTZ conformemente ai limiti indicati nel presente regolamento e, pertanto, senza mai effettuare riprese all'interno di abitazioni o aree private, utilizzando quindi le telecamere solo per il controllo di quanto si svolga nei luoghi pubblici
4. Gli incaricati del trattamento devono operare sui dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del funzionario designato al coordinamento delle attività e al controllo. In ogni caso l'utilizzo degli apparecchi di ripresa da parte degli autorizzati al trattamento dovrà essere sempre conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato.
5. La supervisione dell'impianto di videosorveglianza è attribuita all'Ufficiale responsabile della sala operativa della Polizia Locale.
6. L'acquisizione delle immagini è riservata ad Agenti ed Ufficiali di PG specificatamente individuati ed autorizzati. L'acquisizione delle immagini per le finalità di cui all'art.3, comma 5, è altresì consentita a specifici soggetti espressamente autorizzati dal supervisore dell'impianto.
7. La visione delle immagini è riservata ai soggetti autorizzati. Vengono autorizzati gli operatori della Centrale Operativa, gli operatori del Corpo di Guardia della Polizia Locale di Perugia, eventuali operatori degli uffici decentrati, qualora autorizzati.

Art. 8 Soggetti terzi

1. L'accesso all'impianto è altresì consentito, esclusivamente per le finalità di Istituto alle altre forze di Polizia in relazione al trattamento delle riprese. All'atto dell'accesso i soggetti terzi danno garanzia di osservare le disposizioni previste dal presente regolamento compatibilmente con i rispettivi ordinamenti speciali, nonché in relazione alle disposizioni e agli accessi al sistema di videosorveglianza consentiti dal titolare.

CAPO III - MISURE DI SICUREZZA DELL'IMPIANTO DI VIDEOSORVEGLIANZA

Art. 9 Accesso al sistema di videosorveglianza

1. L'accesso al sistema è esclusivamente consentito al Titolare, al soggetto designato ed ai soggetti autorizzati come indicato negli artt.6, 7 ed 8 del presente regolamento.
2. L'accesso è altresì consentito alle società fornitrici dell'impianto ed a quelle che fanno manutenzione su di esso nei limiti strettamente necessari alle specifiche esigenze di buon funzionamento e manutenzione dell'impianto medesimo ovvero ai soggetti appartenenti al dipartimento servizi tecnologici ed informatici previa individuazione da parte del soggetto responsabile (preventivamente individuato quale sub-designato);
3. la visualizzazione in diretta delle immagini e l'accesso ai dati conservati per la duplicazione su supporto informatico rimovibile per la loro differita visualizzazione è strutturata secondo i seguenti livelli d'accesso:
- A) visualizzazione delle immagini in diretta:
- a1)** accesso utente di primo livello: gli operatori di primo livello detengono la priorità di gestione del sistema. Gli incaricati per la visualizzazione delle immagini in diretta accedono al sistema mediante credenziali di autenticazione abilitanti alla visione delle stesse. Detto personale è nominato con specifico Atto di Nomina del Comandante
- a2)** accesso utente di secondo livello: il personale di cui all'art.8 può gestire tutte le telecamere in modo indipendente tranne quelle in fase di utilizzo dell'operatore con accesso di primo livello di cui al precedente punto.
- a3).** L'accesso alla visualizzazione e gestione delle telecamere da parte degli operatori di secondo livello dovrà essere autorizzato dall'Ufficiale responsabile della Centrale

Operativa di primo livello o comunque dall'operatore addetto al servizio di primo livello che ne informerà l'Ufficiale.

a4) In caso di necessità per manutenzione e assistenza, la ditta incaricata dagli uffici comunali competenti, può accedere alla visualizzazione delle immagini in diretta presso ogni postazione mediante personale tecnico appositamente incaricato ma solo alla presenza dei soggetti autorizzati alla visione delle immagini.

B) visualizzazione differita e duplicazione delle immagini registrate

b1) l'accesso avviene mediante postazioni dedicate posizionate presso la Centrale Operativa della Polizia Locale di Perugia e dei soggetti di cui all'art.8. L'incaricato alla consultazione delle immagini registrate si autentica mediante credenziali di autenticazione abilitanti su apposito software dedicato e accede all'area dell'archivio digitale nella quale ricerca, salva e duplica immagini o filmati esclusivamente per i fini istituzionali di cui all'art.3 del presente regolamento;

b2) In caso di necessità, manutenzione e assistenza, la ditta abilitata al servizio tecnico mediante personale appositamente incaricato, può accedere al sistema di videoregistrazione e alla visualizzazione delle immagini registrate esclusivamente per le suddette necessità e nel rispetto degli obblighi di segretezza e riservatezza. Le operazioni di manutenzione e assistenza necessarie devono essere eseguite solo alla presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini registrate.

4. L'accesso è, inoltre, consentito:

a. 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. 10. L'accesso da parte dell'interessato, sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;

b. ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

5. Non potrà essere concesso laddove riproduca immagini di soggetti terzi, quando non sia possibile esperire la procedura di acquisizione di consenso per difficoltà di identificazione o per l'elevato numero di soggetti coinvolti.

6. Per quanto riguarda l'accesso da parte di privati ai sensi del comma 4 del presente regolamento, verrà richiesto un contributo forfetario destinato a coprire le spese di ricerca ed estrapolazione dei filmati, da determinare con atto a parte.

7. L'accesso ai privati non è consentito laddove si sia instaurato un procedimento penale, anche con denuncia o querela, per il quale legittimata ad acquisire le immagini sarà la Forza di Polizia procedente.

L'accesso è consentito agli avvocati ai sensi degli artt. 391-bis e seguenti del C.p.p.

8. La richiesta di accesso dovrà essere evasa entro 30 giorni dall'acquisizione al protocollo, salvo particolari e non prevedibili esigenze di servizio.

Art. 10 Diritti dell'interessato

1. In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., GDPR, su presentazione di apposita istanza, ha diritto:

a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;

b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;

c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 GDPR, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, GDPR.

2. L'istanza per l'esercizio dei diritti dell'interessato è presentata all'Ufficiale incaricato della supervisione dell'impianto di videosorveglianza il quale, eventualmente previa consultazione con il DPO (Responsabile della Protezione dei dati) dell'Ente, decide in merito.

3. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:

- il luogo, la data e la fascia oraria il più possibile precisa e comunque limitata a 30 minuti, 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.

4. Il supervisore 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 ovvero gli comunicherà le ragioni per cui la visione non è possibile. Qualora, ai sensi dell'art.15, paragrafo 3, GDPR, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, GDPR.

5. 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. 11 Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

1. Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, GDPR ed alle previsioni Decreto Legislativo 101/2018 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE", in attuazione della delega al Governo di cui all'art. 13, L. 163/2017

Art. 12 Norme per la gestione del sistema - Misure di sicurezza

1. I dati raccolti mediante il sistema di videosorveglianza sono protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini. 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.

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

3. In particolare gli uffici comunali competenti e i soggetti nominati responsabili del sistema integrato adottano le seguenti specifiche misure tecniche ed organizzative di sicurezza:

A) Centrale Operativa della Polizia Locale, Corpo di Guardia e locale ospitante il server della videosorveglianza per la sicurezza cittadina:

a1) l'accesso alla Centrale Operativa ove sono presenti i monitor di controllo della videosorveglianza che sono sempre accesi è consentito, oltre al Sindaco o suo delegato, agli appartenenti alla Polizia Locale comandati per lo specifico servizio d'istituto disposto dal Comando. È consentito l'accesso di soggetti incaricati di servizi e funzioni rientranti nei compiti istituzionali del Comune di Perugia. È consentito, altresì, l'accesso al personale addetto alla manutenzione degli impianti e alla pulizia dei locali, i cui nominativi devono essere comunicati per iscritto al Comando. Eventuale accesso di altri e diversi soggetti deve essere appositamente autorizzato per iscritto dal Comandante. L'accesso al sistema di videosorveglianza degli operatori del Corpo di Guardia è regolamentato allo stesso modo di quelli della Centrale Operativa, ad esclusione dell'extrapolazione immagini. Le postazioni di visualizzazione sono in front office e nel locale retrostante. I monitor del front office sono protetti da un pannello oscurante per evitare la visualizzazione da parte degli utenti.

a2) i monitor di controllo della videosorveglianza che sono sempre accesi si trovano all'interno della Centrale Operativa ove la porta d'ingresso rimane chiusa e l'ingresso al locale è gestito dagli operatori.

a3) l'accesso al locale chiuso a chiave che ospita il server della videosorveglianza è consentito a soggetti autorizzati e previa registrazione dell'accesso nell'apposito registro.

B) I soggetti di cui all'art.8 adottano idonee e specifiche misure tecniche ed organizzative di sicurezza in relazione ai rispettivi ordinamenti speciali. L'accesso al sistema di videosorveglianza è tracciato ed archiviato elettronicamente.

C) Misure tecniche di sicurezza generale del sistema di videosorveglianza:

c1) nessuna postazione di videosorveglianza può anche accidentalmente cancellare ovvero distruggere quanto registrato nel server;

c2) il software di gestione deve governare l'accesso al sistema di videosorveglianza con credenziali di autenticazione abilitanti, attraverso l'utilizzo autenticazione basata su nome utente e password di accesso;

c3) la cronologia degli eventi di accesso al sistema videosorveglianza deve essere archiviata elettronicamente per almeno sei mesi;

c4) l'accesso ai server è dotato di "log" di accesso, che saranno conservati per la durata di anni uno;

c5) le credenziali per gli accessi al sistema di videosorveglianza devono essere disattivate in caso di mancato utilizzo per un periodo di sei mesi o in caso di perdita dell'incarico che consenta al soggetto l'accesso al sistema di videosorveglianza;

- c6)** nel server deve essere garantito un livello di duplicazione di sicurezza dei dati, tale duplicazione di dati dovrà anch'essa sottostare, riguardo il periodo di conservazione, alle disposizioni normative vigenti in materia di protezione dei dati personali;
- c7)** tutti gli apparati esterni devono essere monitorati da personale tecnico incaricato a cui compete segnalare costantemente e tempestivamente ogni anomalia e manomissione
- c8)** la telecomunicazione ed il trasporto delle informazioni deve avvenire con sistema di crittografia avente idonee chiavi di cifratura che escludono ogni accesso abusivo;
- c9)** i punti di ripresa devono sospendere automaticamente ogni trasmissione del dato in caso di manomissione e/o accesso abusivo al sistema.
- c10)** l'eventuale cancellazione delle immagini registrate sarà possibile solo per soddisfare i diritti degli interessati di cui all'art.10.
- D)** Casi particolari: in alcuni specifici casi, per ragioni tecniche e/o di sicurezza relativa ad impianti periferici, i dati vengono registrati, su DVR/NVR locali. In questi casi i sistemi di salvataggio dei dati sono posizionati in modo non accessibile e sono protetti da password.

CAPO IV - TRATTAMENTO DEI DATI PERSONALI SICUREZZA E LIMITI ALLA UTILIZZABILITA' DEI DATI

Art. 13 Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento sono:
 - a) trattati in modo lecito e secondo correttezza;
 - b) raccolti e registrati per le finalità di cui agli artt.3 e 4 del presente regolamento e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni compatibili con tali scopi, esatti e, se necessario, aggiornati;
 - c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
 - d) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per i quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dal successivo comma 5 del presente articolo.
2. I dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza, installate sul territorio comunale in relazione alle esigenze di prevenzione generale, ordine e sicurezza pubblica indicate dall'Autorità di Pubblica Sicurezza.
3. Gli apparati di ripresa e i software devono funzionare con dei preset o altri accorgimenti idonei che evitano, durante la cosiddetta funzione di tour automatico, la ripresa dell'interno delle finestre degli edifici o di luoghi privati.
4. Le telecamere consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario. I segnali video delle telecamere sono inviati in tempo reale alle Centrali Operative delle varie forze di Polizia per essere visualizzate sui monitor. Tutti i segnali video delle telecamere sono registrati su un apposito server collocato in un idoneo locale presso il Comune di Perugia e/o su DVR/NVR. L'impiego del sistema di conservazione delle registrazioni video è necessario per ricostruire gli eventi in relazione alle finalità previste dal presente regolamento.
5. Le registrazioni video sono conservate, per un tempo non superiore a sette giorni successivi alla rilevazione, presso il server di sistema che consente di aderire alle finalità indicate all'art.4 del presente regolamento salvo specifiche richieste investigative dell'autorità giudiziaria o della polizia giudiziaria. Lo stesso intervallo temporale si applica ai dati presenti sui DVR/NVR. Decorso il suddetto termine di sette giorni le immagini riprese in tempo reale sovrascrivono quelle registrate.
6. In caso di cessazione per qualsiasi causa di un trattamento i dati personali sono:
 - a) distrutti;

b) eccezionalmente conservati in relazione a procedimenti connessi alle finalità di cui all'art.3 del presente regolamento.

Art. 14 Informazioni rese al momento della raccolta

1. Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).

2. A tal fine l'Ente utilizzerà, per i nuovi cartelli da installare, lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, riportato in fac-simile nelle già richiamate linee guida in materia di videosorveglianza e di seguito riportato, con indicazione, nel lato inferiore del cartello, il riferimento normativo "Art. 13 del Regolamento europeo sulla protezione dei dati personali (RGDP 2016/679).

Il cartello informativo è composto da diverse sezioni:

- Titolo:** Videosorveglianza!
- QR code:** Un codice QR che, quando scansionato, porta all'informatica completa.
- Informazioni obbligate dal GDPR:**
 - Identità del titolare del trattamento:** - nome, ragione sociale, del suo rappresentante
 - Responsabile del responsabile della protezione dei dati (ove applicabile):**
 - Informazioni sul trattamento:** - che ha il maggior impatto sull'interessato - (ad esempio, periodo di conservazione, o monitoraggio in tempo reale, pubblicazione, o trasmissione all'estero a soggetti terzi)
 - Scopo/i della videosorveglianza:**
 - Diritti degli interessati:** - Gli interessati possono esercitare diversi diritti (tra cui, in particolare, il diritto di accedere al titolare del trattamento, l'accesso o la cancellazione dei propri dati personali).
 - Per maggiori dettagli:** - sulla videosorveglianza, compresi i diritti e le necessità, si possono trovare informazioni sul sito del titolare del trattamento, utilizzando l'equivalente elettronico delle cartelle.

Negli altri spazi verranno riportati gli estremi del regolamento, l'identità del Titolare e la casella mail di contatto del DPO e del referente per la videosorveglianza mentre nel QR code sarà contenuto il link per collegarsi al testo completo dell'informatica.

Al fine di garantire una piena tutela al diritto dell'interessato ad essere informato prima di accedere all'area videosorvegliata, detti cartelli verranno collocati nei pressi delle aree videosorvegliate. I cartelli esistenti, fino alla loro sostituzione, vengono considerati idonea a fornire le informazioni necessarie secondo gli obblighi di Legge.

CAPO V ALTRI TRATTAMENTI

Art. 15 impianto di videosorveglianza non pubblico

1. L'impianto di videosorveglianza installato da un privato, deve essere progettato e realizzato in modo da consentire di realizzare già in fase di sviluppo i principi della proporzionalità, della buona fede e della trasparenza. Più precisamente:

a) La videocamera deve essere installata in modo da limitare l'angolo visuale delle riprese alle sole immagini indispensabili per raggiungere le finalità perseguite (principio della proporzionalità).

2. Il privato che intende avvalersi di un impianto di videosorveglianza può utilizzarlo, di regola, solo sul proprio terreno. Il terreno adiacente può essere ripreso soltanto se il vicino ha dato il proprio consenso. Lo stesso vale per le case plurifamiliari con appartamenti in affitto o in proprietà. Anche in questo caso un inquilino o un proprietario possono sorvegliare unicamente le parti di cui ha l'uso esclusivo. La ripresa delle aree comuni presuppone il consenso di tutti gli inquilini dell'immobile. Occorre inoltre considerare che per la ripresa su suolo pubblico si applicano regole particolari.

3. Il proprietario o l'inquilino di un appartamento può riprendere la propria abitazione, incluso il balcone. La videosorveglianza dell'area di ingresso, della tromba delle scale (pianerottoli compresi), della lavanderia o del garage è possibile solamente con il consenso di tutti.

4. I responsabili della videosorveglianza devono informare con un cartello ben visibile conforme al modello, tutte le persone che entrano nel campo controllato che in quel luogo si effettua videosorveglianza. Se le immagini riprese sono collegate a un archivio di dati – ossia se vengono in qualche modo memorizzate - occorre indicare anche da chi si può far valere il diritto di accedervi se ciò non si evince dal contesto (principio della buona fede e diritto d'accesso).

5. Censimento impianti di videosorveglianza attivi nel territorio comunale

I titolari di impianti di videosorveglianza attivi nel territorio comunale sono obbligati a comunicare al Comune di Perugia, entro 60 giorni dalla loro installazione, i principali dati riferibili a detti impianti, in particolare:

- ubicazione dell'impianto;
- dati identificativi e reperibilità del titolare dell'impianto;
- dati identificativi e reperibilità del responsabile del trattamento.

La comunicazione dei predetti dati sarà effettuata con modalità semplificate mediante il loro inserimento nella sezione dedicata predisposta sul sito internet comunale, visionabile esclusivamente dalle Forze di Pubblica Sicurezza.

Con le stesse modalità e nello stesso termine di 60 giorni, il titolare dell'impianto dovrà comunicare eventuali variazioni dei dati precedentemente comunicati.

Sono esclusi dall'obbligo di comunicazione gli impianti attivi all'interno di aree private.

Eventuali violazioni alle norme contenute nel presente articolo sono contestate dagli organi di controllo nei modi e nei termini previsti dalla legge 24.11.1981 n. 689 e ss. mm. ii. e sono punite, ai sensi dell'art. 7 bis del D. Lgs. 267/2000, con la sanzione amministrativa da € 50,00 ad € 500,00.

Art. 16 Sicurezza cittadina

1. Per tutte le nuove lottizzazioni, sarà possibile per i lottizzanti, installare un sistema di videosorveglianza, collegabile al sistema comunale, che riprenda gli accessi alle lottizzazioni sia in entrata sia in uscita, segnalando l'esistenza del sistema di videosorveglianza, al fine di scoraggiare eventuali malintenzionati e garantire contestualmente sicurezza ai residenti.

2. Nell'ambito di progetti di sicurezza partecipata, l'accesso all'impianto, in modalità di visione, può, inoltre essere concesso, sulla base di specifica autorizzazione nominale ad opera del supervisore dell'impianto, a specifici soggetti debitamente formati appartenenti ad associazioni operanti sul territorio. Il presente comma potrà essere attuato solo successivamente l'adozione di specifica regolamentazione dei progetti di sicurezza partecipata da parte del Comune di Perugia.

3. Il personale del Corpo di Polizia Locale può utilizzare, per i servizi individuati dall'Amministrazione, dispositivi ulteriori di ripresa, come BodyCam (telecamere posizionate direttamente sulle divise degli operatori di P.L.), DashCam (telecamere a bordo di veicoli di servizio), in conformità delle indicazioni dettate dal Garante per la protezione dei dati personali con nota 26 luglio 2016, prot. 49612, con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi, ed il cui trattamento dei dati viene ricondotto a "dati personali direttamente correlati all'esercizio di compiti di

polizia, di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria”.

4. In relazione all'utilizzo di BodyCam e Dashcam, il Comando del Corpo tiene uno specifico disciplinare interno, da rendere obbligatorio per operatori di Polizia Locale, con indicazione delle casistiche di attivazione di tali strumenti, dei soggetti eventualmente autorizzati a disporre l'attivazione, delle operazioni autorizzate in caso di emergenza e di ogni altra misura organizzativa e tecnologica necessaria alla corretta e legittima gestione di detti dispositivi.

5. Al fine di conseguire una maggiore diffusione delle iniziative di sicurezza urbana nel territorio, nonché per ulteriori finalità di interesse pubblico, il Comune favorisce la realizzazione di progetti proposti da enti gestori di edilizia residenziale ovvero da amministratori di condomini, da imprese, anche individuali, da associazioni di categoria ovvero da consorzi o da comitati comunque denominati all'uopo costituiti fra imprese, professionisti o residenti per la messa in opera a carico di privati di sistemi di sorveglianza tecnologicamente avanzati, dotati di software di analisi video per il monitoraggio attivo con invio di allarmi automatici a centrali delle forze di polizia o di istituti di vigilanza privata convenzionati

6. Il Comune potrà stipulare accordi con specifici soggetti quali, a mero titolo di esempio, mobilità urbana, trasporto pubblico o privato al fine di agevolare, anche mediante contributi, l'acquisto e l'installazione di DASHCAM a bordo dei veicoli. Tali dispositivi dovranno essere dotati di apposita fessura per l'inserimento di una memoria di massa di registrazione, ad esempio una “micro SD”, essenziale per registrare i filmati, accesso ai filmati tramite connessione wireless e registrazione della posizione GPS del veicolo al momento della ripresa. I filmati potranno essere richiesti per finalità di pubblica sicurezza, di polizia giudiziaria o ricostruzione di sinistri e potranno essere richiesti al cittadino o spontaneamente consegnati da questi.

7. Al di fuori di quanto previsto nei commi precedenti, il privato che si trovi a documentare con strumenti di ripresa visiva o sonora fatti giuridicamente rilevanti può consegnarne copia al Corpo di Polizia locale mediante procedura che garantisca la riconducibilità del filmato all'autore originario e mediante sottoscrizione di apposita dichiarazione.

Art. 17 Rilevamento infrazioni al CdS

1. Il Comune utilizza dispositivi elettronici per la rilevazione di violazioni al Codice della strada. Detti impianti vengono utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale e, analogamente all'utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.

2. Nell'utilizzo di tali sistemi vengono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate. In conformità alla prassi ed al quadro normativo di settore riguardante talune violazioni del Codice della strada si richiamano le prescrizioni del Garante:

a) gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;

b) le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (es., ai sensi dell'art. 383 del d.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento amministrativo (es., pedoni, altri utenti della strada);

- c) le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;
- d) le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;
- e) le fotografie o le immagini che costituiscono fonte di prova per le violazioni contestate non devono essere inviate d'ufficio al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;
- f) in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e, pertanto, di ottenere dalla competente autorità ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.

3. I conducenti dei veicoli e le persone che accedono o transitano in aree dove sono attivi sistemi elettronici di rilevazione automatizzata delle violazioni devono essere previamente informati in ordine al trattamento dei dati personali.

4. Per quanto riguarda i sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, verranno rispettate le previsioni previste dal d.P.R. 22 giugno 1999, n. 250: i dati trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso, ferma restando l'accessibilità agli stessi per fini di polizia giudiziaria o di indagine penale (art. 3 d.P.R. n. 250/1999).

CAPO VI DISPOSIZIONI FINALI

Art. 18 Modifiche regolamentari e ampliamento del sistema

1. I contenuti del presente regolamento dovranno essere aggiornati nei casi di modifiche normative in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità Garante dei dati personali o atti regolamentari generali del Consiglio Comunale dovranno essere immediatamente recepiti.

2. L'ampliamento del numero delle postazioni delle telecamere di videosorveglianza, per la sicurezza cittadina, di cui alle finalità previste dall' art.3 del presente regolamento, nonché integrazioni di nuovi client, è deliberato dalla Giunta Comunale.

3. L'individuazione delle postazioni delle telecamere di cui al comma 2 è demandata agli uffici comunali competenti, prioritariamente in relazione alle esigenze di prevenzione generale, ordine e sicurezza pubblica indicate dall'Autorità di Pubblica Sicurezza.

4. L'integrazione al sistema di ulteriori Centrali Operative, al di fuori di quelle sopra indicate, saranno trattate come utenti di secondo livello e varrà quanto indicato negli artt. 7, 8 e 9 del presente regolamento.

Art. 19 Rinvii ed abrogazioni

1. Per quanto non disciplinato dal presente regolamento si rinvia alle norme legislative e regolamentari vigenti in materia.

2. Ogni altra disposizione regolamentare antecedente nonché contraria o incompatibile con il presente regolamento in materia di videosorveglianza del territorio cittadino si deve intendere abrogata. In particolare l'art.30 del Regolamento di Polizia Urbana approvato con deliberazione del Consiglio Comunale n. 182 del 12.12.2011 è sostituito dal comma 5 del precedente art.15.

Art. 20 Entrata in vigore e pubblicazione

1. Il presente regolamento entra in vigore dopo la pubblicazione ai sensi di legge all'Albo Pretorio Comunale online ed è trasmesso al Garante per la protezione dei dati personali ed ai soggetti di cui all'art.8.

2. Copia del regolamento è tenuta a disposizione del pubblico presso le URP cittadine ed i Comandi zona. Il documento è altresì pubblicato sul sito internet del Comune di Perugia.

FAC-SIMILE del modulo per istanza di accesso ai filmati da parte di privato

Premesso che,

- l'articolo 9, comma 4, del Regolamento comunale del sistema di videosorveglianza prevede espressamente che:

4. L'accesso è, inoltre, consentito

a. 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. 10. L'accesso da parte dell'interessato, sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;

b. ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

- l'articolo 9, comma 5, del Regolamento comunale del sistema di videosorveglianza prevede espressamente che:

5. Per quanto riguarda l'accesso da parte di privati ai sensi del comma 4 del presente regolamento, potrà essere richiesto un contributo forfetario destinato a coprire le spese di ricerca ed estrapolazione dei filmati.

Il sottoscritto _____, nato a _____, il _____ e residente in _____, via _____, identificato a mezzo _____ nr _____

consapevole delle sanzioni previste per chiunque renda false dichiarazioni all'Autorità, chiede a questo Spett.le Corpo Polizia Municipale di Perugia – Centrale Operativa PEC _____

Chiede nella sua qualità di

interessato del trattamento ai sensi dell'art.4, n°1 del Regolamento Europeo in materia di protezione dei dati personali 2016/679 (GDPR)¹;

A) La verifica dell'esistenza di riprese che lo riguardino nei filmati effettuati in data _____ dalle ore ____ alle ore ____ in via _____;

a. con estrazione della copia

b. senza estrazione di copia

Fornisce le seguenti informazioni:

- il luogo, la data e la fascia oraria il più possibile precisa e comunque limitata a 30 minuti, della possibile ripresa;
- l'abbigliamento indossato al momento della possibile ripresa;

¹ Ai sensi dell'art.4 GDPR «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

Ai sensi dell'art.9, comma 5, si allega copia della ricevuta del versamento di

euro _____ per la ricerca dei fotogrammi

euro _____ per l'acquisizione dei fotogrammi

Data _____

Firma del richiedente

Il rilascio di quanto richiesto è subordinato al pagamento dell'importo stabilito con atto a parte, secondo modalità da determinare, da effettuare tramite:

versamento con bollettino postale su CCP n. 00005066 intestato a Comune di Perugia Comando Vigili Urbani Uff Contravvenzioni- Servizio Tesoreria; causale Proventi derivanti da richieste immagini videosorveglianza;

bonifico bancario UNICREDIT SPA Agenzia di Perugia->Corso Vannucci 39 IBAN IT07D0200803027000029502587 avendo cura di specificare quanto riportato nel punto precedente

Data _____

Firma del richiedente

In data _____ considerata la suddetta richiesta e l'autorizzazione del responsabile si è proceduto alla estrazione delle immagini e alla relativa consegna

Firma dell'incaricato

Firma del richiedente

FAC-SIMILE del modulo per comunicazione dei dati

Spett.le _____
(indirizzare al titolare o al responsabile del trattamento)

Oggetto: comunicazione dei dati al Soggetto pubblico, all'Autorità Giudiziaria o alla Polizia Giudiziaria

In data _____ alle ore _____ il sottoscritto _____ appartenente a _____

Chiede

l'estrazione di immagini dal sistema di videosorveglianza installato per fini di ordine e sicurezza pubblica:

per fini di ordine e sicurezza pubblica;
per specifica richiesta dell'autorità giudiziaria;
in relazione all'attività investigativa in corso.

Nell'avanzare la presente richiesta rilascia le seguenti informazioni:

data della ripresa video _____; fascia oraria _____; luogo della ripresa video _____

Data _____

Firma del richiedente

In data _____ considerata la suddetta richiesta e l'autorizzazione del responsabile si è proceduto alla estrazione delle immagini e alla relativa consegna

Firma dell'incaricato

Firma del richiedente

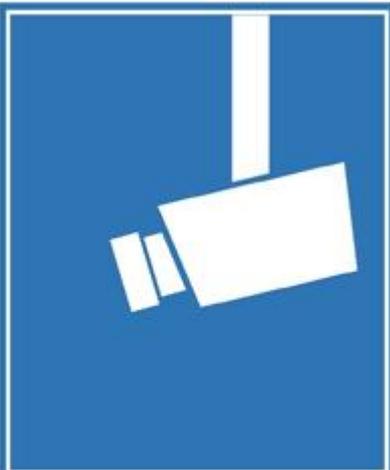
Data_____

Firma del dichiarante

(Se nel corso dell'esame emergono indizi di reità a carico dell'esponente:

«A questo punto, poiché dalle dichiarazioni sopra rese emergono a carico dello stesso dichiarante indizi di reità in ordine al reato per cui si procede, l'interrogatorio viene sospeso ed il Sig. _____ viene invitato a nominarsi un difensore»

L'atto viene chiuso e si procederà, procurata la presenza del difensore di fiducia o di ufficio, secondo lo schema di verbale di sommarie informazioni dalla persona sottoposta alle indagini ex art. 350 c.p.p.)



Videosorveglianza!

Identità del titolare:
[Titolare trattamento]

Dati di contatto del responsabile della protezione dei dati:
[DPO]

Finalità del trattamento cui sono destinati i dati personali nonché la base giuridica per l'elaborazione:
Controllo in tempo reale senza memorizzazione per prevenire furti o atti vandalici. Registrazione delle immagini per perseguire gli autori di furti o atti vandalici.

Diritti degli interessati:
*In qualità di interessato godete di diversi diritti nei confronti del titolare del trattamento, in particolare il diritto di richiedere al responsabile del trattamento l'accesso o la cancellazione dei vostri dati personali.
Per i dettagli su questa videosorveglianza, compresi i vostri diritti, consultate le informazioni complete fornite dalla attraverso le opzioni presentate a sinistra.*

Ulteriori informazioni:


Telecamera 1, telecamera 2, telecamera piazzale anteriore, ...

Telecamere a protezione perimetrale, telecamere a protezione ingresso via ...

La data dell'ultima revisione dell'informazione estesa è ...

- PRIMA CASELLA: dati di contatto del titolare
- SECONDA CASELLA: dati di contatto del DPO
- TERZA CASELLA: finalità del trattamento
- QUARTA CASELLA: diritti degli interessati
- QR code: link al regolamento