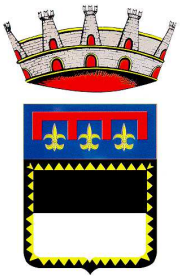

COMUNE DI CESENA

Codice per il trattamento dei dati personali e la videosorveglianza

PARTE I - Approvata con Deliberazione di Consiglio comunale n. 14 del 21/03/2019
in vigore dal 13/04/2019

PARTE II - Approvata con Deliberazione di Consiglio comunale n. 5 del 31/01/2019
in vigore dal 19/02/2019

INDICE

PARTE I
REGOLAMENTO PER L'ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

CAPO I – DISPOSIZIONI GENERALI

Articolo 1 – Oggetto

1. Il presente regolamento disciplina le misure organizzative ed i processi interni in materia di trattamento dei dati personali delle persone fisiche nell'ambito delle funzioni e finalità istituzionali del Comune di Cesena, in attuazione del Regolamento europeo (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"*, (di seguito anche "GDPR o Regolamento europeo") e del D.Lgs.30 giugno 2003, n. 196 *"Codice in materia di protezione dei dati personali"*, (di seguito anche "Codice"), modificato dal D.Lgs.10 agosto 2018, n. 101, recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"*.

2. Ai fini del presente regolamento, si intendono per funzioni istituzionali:

- le funzioni previste dalla legge, dallo Statuto, dai regolamenti e dalla normativa comunitaria;
- le funzioni svolte per mezzo di intese, accordi di programma e convenzioni nelle materie attribuite alla competenza del Comune di Cesena.

Articolo 2 – Finalità del trattamento

1. I dati personali sono trattati dal Comune di Cesena, nel rispetto dei principi sanciti dall'art. 5 del Regolamento (UE) 2016/679, per le seguenti finalità istituzionali:

a) l'adempimento di un obbligo legale al quale è soggetto l'Ente in qualità di Titolare del trattamento;
b) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:
    - l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
    - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale, regionale, provinciale, attribuite all'Ente in base alla vigente legislazione;

c) l'esecuzione *ex lege* di un contratto o misure precontrattuali con gli interessati;
d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento dei propri dati personali.

Art. 3 – Ambito di applicazione

1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in uno o più archivi o destinati a figurarvi del Comune di Cesena.

2. Il presente regolamento non si applica ai trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse ai sensi dell'art. 2, paragrafo 2, lett. d), del Regolamento (UE) 2016/679; per detti trattamenti trova applicazione il D.Lgs. 18 maggio 2018 n. 51 recante *"Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio"*.

Articolo 4 – Definizioni

1. Ai fini del presente regolamento s'intende per:

- **dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **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;
- **trattamento su larga scala:** trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché altri trattamenti che presentano un rischio

elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti;

- **profilazione:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **pseudonimizzazione:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **archivio:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **titolare del trattamento:** il Comune di Cesena, in persona del Sindaco *pro-tempore,* ovvero, 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;
- **contitolare del trattamento:** due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali;
- **responsabile del trattamento:** i Settori rappresentati organicamente dal loro Dirigente, ovvero, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **destinatario:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione Europea o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- **terzo:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **consenso dell'interessato:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante

dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

- **violazione dei dati personali:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **dati biometrici:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **dati relativi alla salute:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento (UE) 2016/679 ovvero il Garante per la protezione dei dati personali;
- **rappresentante:** la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- **D.P.I.A.:** è la "Valutazione di Impatto sulla Protezione dei Dati" ovvero quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati particolare, o anche per una combinazione di questi e altri fattori), il Regolamento (UE) 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti , cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato;
- **Codice:** il Decreto Legislativo 30 giugno 2003 n. 196 recante il "Codice in materia di protezione dei dati personali", modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
- **GDPR o Regolamento Europeo:** il *"General Data Protection Regulation"*, ovvero, il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (regolamento generale sulla protezione dei dati).

CAPO II - SOGGETTI DEL TRATTAMENTO

Articolo 5 – Titolare del trattamento

1. Il Titolare del trattamento dati è il Comune di Cesena, rappresentato dal Sindaco *pro-tempore*, (di seguito indicato anche "Titolare").

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'articolo 5 del Regolamento (UE) 2016/679:

- liceità;
- correttezza e trasparenza;
- limitazione della finalità;
- minimizzazione dei dati, esattezza;
- limitazione della conservazione;
- integrità e riservatezza.

3. La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del Regolamento europeo. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento europeo. Dette misure sono riesaminate e aggiornate qualora necessario.

4. Le misure sono definite fin dalla fase di progettazione e messe in atto per ridurre al minimo il trattamento dei dati personali e applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

5. Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'articolo 13 del GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
b) le informazioni indicate dall'articolo 14 del GDPR, qualora i dati personali non sono stati ottenuti presso lo stesso interessato.

6. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "D.P.I.A.") ai sensi dell'articolo 35 e ss. del GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

7. Il Titolare provvede a:

a) designare i Responsabili del trattamento dati, individuati:
   - nei servizi ovvero nei Settori dell'Ente, rappresentati organicamente dal Dirigente

preposto all'unità organizzativa competente;

- nei soggetti pubblici o privati, affidatari di attività e servizi per conto del titolare, relativamente alle banche dati gestite da soggetti esterni all'Ente, in virtù di convenzioni, contratti, incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali; per dette designazioni il Titolare autorizza direttamente i Settori dell'Ente (responsabili "interni") alla nomina di Responsabili "esterni" in ragione delle specifiche attività di controllo verso codesti soggetti.

b) nominare il Responsabile della protezione dei dati (RPD-DPO) *ex* art. 37 e ss. del GDPR.

8. Il titolare del trattamento deve verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare dall'art. 28, paragrafo 3, del Regolamento europeo.

9. Il titolare del trattamento deve valutare l´esistenza di eventuali situazioni di contitolarità, essendo obbligato in tal caso a stipulare l´accordo interno di cui all´art. 26, paragrafo 1, del GDPR.

Articolo 6 – Contitolari del trattamento

1. La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.

2. Nell'ambito dell'esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune di Cesena dall'Unione dei Comuni "Valle del Savio" (a cui aderiscono i Comuni di Cesena, Bagno di Romagna, Mercato Saraceno, Montiano, Sarsina, Verghereto), da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'articolo 26 del GDPR.

3. Il Comune di Cesena e l'Unione dei Comuni "Valle del Savio", sono da considerarsi, pertanto, ognuno per le proprie rispettive attribuzioni *ex* artt. 13 e 14 D.Lgs. 18 agosto 2000, n. 267, nonché per effetto di convenzioni ed accordi, Titolari o Contitolari del trattamento dei dati personali.

4. L'accordo di contitolarità:

a) definisce le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento Europeo, con particolare riferimento all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando quanto eventualmente stabilito dalla normativa specificatamente applicabile;

b) può designare un punto di contatto comune per gli interessati;

c) riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato, ai fini dell'esercizio dei diritti previsti dagli articoli 15 e ss. del GDPR. Indipendentemente dalle disposizioni di tale accordo, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento.

Articolo 7 – Responsabile del trattamento

1. Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

2. Il titolare si avvale di Responsabili "interni" individuati nel Settore amministrativo/tecnico dell'Ente cosi come rappresentati dal Dirigente preposto e di Responsabili "esterni" in virtù di specifico contratto/convenzione a sua volta designati dai Responsabili "interni" competenti sulla base di espressa previsione regolamentare richiamata all'art. 5.

3. Il Responsabile del trattamento, che tratta i dati personali per conto del Titolare del trattamento, deve rispettare pienamente quanto previsto dalle leggi vigenti e dalle disposizioni del regolamento europeo in materia di trattamento e sicurezza dei dati personali.

4. Il Responsabile del trattamento procede alla designazione degli incaricati ovvero delle **persone autorizzate al trattamento** dei dati personali che si impegnano alla riservatezza e che assumono pertanto un obbligo legale di riservatezza. La nomina delle persone autorizzate al trattamento avviene mediante atto scritto, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi ed i diritti del Titolare del trattamento.

La nomina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun responsabile designato.

5. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'articolo 28 del Regolamento (UE) 2016/679.

6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

7. Il Regolamento europeo consente la nomina di **sub-responsabili** del trattamento da parte di ciascun responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile "primario"; le operazioni di trattamento possono essere effettuate solo da persone autorizzate che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificamente l'ambito del trattamento consentito.

8. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte

le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, in particolare:

- alla tenuta del registro delle attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- ad assistere il Titolare nella conduzione della D.P.I.A. fornendo allo stesso ogni informazione di cui è in possesso;
- alla designazione di un Responsabile della protezione dati (RPD-DPO) nei casi previsti dal regolamento europeo o dal diritto nazionale, se a ciò demandato dal Titolare del trattamento *(art. 37 GDPR)*;
- in caso di violazione dei dati personali ad informare il Titolare, senza ingiustificato ritardo, ed in ogni caso entro 24 ore dal momento in cui ne è venuto a conoscenza (cd. *"data breach"*), per consentire al Titolare la notificazione al Garante per la protezione dei dati personali, entro i termini previsti dall'art. 33, comma 1, del Regolamento (UE) 2016/679, ovvero, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Articolo 8 - Responsabile della protezione dati

1. Il Titolare del Trattamento procede alla nomina del Responsabile della protezione dei dati (RPD-DPO) *ex* art. 37 e ss. del GDPR. Il Titolare o il Responsabile del trattamento provvede alla pubblicazione dei dati di contatto del DPO ed alla comunicazione del nominativo al Garante per la protezione dei dati personali in conformità all'articolo 37, paragrafo 7, del Regolamento. Questa disposizione mira a garantire che l'autorità di controllo possa contattare il Responsabile della Protezione dei Dati in modo facile e diretto. In base all'articolo 39, paragrafo 1, lettera e), del GDPR, il Responsabile della Protezione dei Dati funge da punto di contatto fra l'Ente e il Garante.
2. Il R.P.D. è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il R.P.D. può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, ed a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
b) sorvegliare sull'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del

trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;
d) fornire, se richiesto, un parere in merito alla D.P.I.A. e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il R.P.D. in merito a:
   - se condurre o meno una D.P.I.A.;
   - quale metodologia adottare nel condurre una D.P.I.A.;
   - se condurre la D.P.I.A. con le risorse interne ovvero esternalizzandola;
   - quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
   - se la D.P.I.A. sia stata condotta correttamente o meno e se le conclusioni raggiunte siano conformi al GDPR;
e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del R.P.D. è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;
f) verificare la tenuta dei registri delle attività e delle categorie di trattamento, sotto la responsabilità del Titolare del trattamento.

3. Il Titolare ed il Responsabile del trattamento assicurano che il R.P.D. sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il R.P.D. è invitato a partecipare alle riunioni di coordinamento del Dirigenti e/o Responsabili di P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il R.P.D. deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del R.P.D. sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta dall'Ente determini condotte difformi da quelle raccomandate dal R.P.D., è necessario motivare specificamente tale decisione;
- il R.P.D. deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

4. Il R.P.D. è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, che il Titolare potrà garantire, compatibilmente con le risorse di Bilancio, qualora la disciplina dello specifico rapporto preveda tale tipo d'intento, con onere di comunicazione di detto adempimento al Titolare ed al Responsabile del trattamento.

5. Nello svolgimento dei compiti affidatigli il R.P.D. deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il R.P.D.:

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività-, incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

6. Il R.P.D. dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

7. La figura di R.P.D. è incompatibile con chi determina le finalità od i mezzi del trattamento. In particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Responsabile del trattamento;
- qualunque incarico o funzione che comporti la determinazione di finalità o mezzi del trattamento.

8. Il Titolare ed il Responsabile del trattamento forniscono al R.P.D. le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al R.P.D.:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (D.U.P.), di bilancio, di Peg e di Piano della performance;
- tempo sufficiente per l'espletamento dei compiti affidati al R.P.D.;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero tramite la costituzione di una U.O., ufficio o gruppo di lavoro R.P.D. (formato dal R.P.D. stesso e dal rispettivo personale);
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

9. Il Responsabile della protezione dati:

a) opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti. In particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare ad una specifica questione attinente alla normativa in materia di protezione dei dati;
b) non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di

detti compiti, il R.P.D. riferisce direttamente al Titolare od al Responsabile del trattamento.

10. Nel caso in cui siano rilevate dal R.P.D. o sottoposte alla sua attenzione decisioni incompatibili con il Regolamento Europeo, con altre norme dell'ordinamento e/o con le indicazioni fornite dallo stesso R.P.D., quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

CAPO II - SICUREZZA DEL TRATTAMENTO

Articolo 9 - Sicurezza del trattamento

1. L'art. 5, par. 1, lett. f), del Regolamento (UE) 2016/679 stabilisce che i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza degli stessi, compresa la protezione, mediante misure tecniche e organizzative adeguate, a garanzia degli obblighi di integrità e disponibilità dei dati. Tale obbligo è richiamato negli articoli 24, 28 e da 32 a 34 del Regolamento europeo e tale valutazione sarà rimessa, caso per caso, al titolare, contitolare e al responsabile, in rapporto ai rischi specificamente individuati dall'art. 32 del regolamento europeo, tenendo conto dei seguenti elementi:

- lo stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche 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, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale;
- la notificazione della violazione dei dati nel rispetto delle tempistiche previste dagli artt. 33 e 34 del GDPR e la comunicazione all'interessato, senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

2. Il rischio per i diritti e le libertà delle persone fisiche inerente al trattamento, costituisce uno degli elementi da considerare per valutare l'adeguatezza delle misure tecniche ed organizzative. Le Linee Guida del *Gruppo di Lavoro Articolo 29*, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017, concernenti *"la valutazione di impatto nonché i criteri per stabile se il trattamento possa presentare un rischio elevato"*, precisano che per "rischio" s'intende uno scenario descrittivo di un evento e delle relative conseguenze che sono stimate in termini di gravità e probabilità. I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da

segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;

- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

3. La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato (C76).

4. L'adeguatezza delle misure di sicurezza deve ricomprende, pertanto, tra le altre, se del caso:

a) l'adozione di tecniche di pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

5. Il titolare e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare, poiché costituisce una misura di sicurezza anche l'istruzione delle persone autorizzate al trattamento, ai sensi dell'art. 32, paragrafo 4, del Regolamento europeo.

Articolo 10 - Registri delle attività di trattamento

1. Il Comune di Cesena si avvale di una piattaforma software per la tenuta, in formato elettronico, dei registri di trattamento secondo le indicazioni dettate dalla normativa vigente.

2. L'art. 30 del GDPR dispone, infatti, l'obbligo per ogni titolare e responsabile del trattamento di tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49 del GDPR, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, paragrafo 1, del Regolamento (UE) 2016/679.

3. Su richiesta, il titolare del trattamento o il responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Articolo 11 - Valutazioni d'impatto sulla protezione dei dati

1. La Valutazione d'impatto sulla protezione dei dati (D.P.I.A.) è un processo previsto nei casi di trattamento che prevede l'uso di nuove tecnologie o quando trattasi di trattamento di nuovo tipo e per i quali il titolare del trattamento non ha ancora effettuato alcuna DPIA, o quando l'esecuzione della D.P.I.A. sia necessaria alla luce del tempo trascorso dal trattamento iniziale.

2. Gli articoli 35 e 36 del GDPR prevedono che, quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento stesso, possa presentare un rischio elevato per i diritti e le persone fisiche, il titolare del trattamento proceda, prima di effettuare il trattamento stesso, alla predisposizione della D.P.I.A.

3. Il Titolare del trattamento:

a) è responsabile dello svolgimento di una preventiva D.P.I.A. per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione deve essere preso in considerazione nella determinazione delle opportune misure tecniche ed organizzative da adottare per dimostrare che il trattamento dei dati personali rispetta il regolamento europeo;
b) sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento, nei casi in cui la D.P.I.A. riveli la presenza di rischi residui elevati che non possono essere attenuati mediante l'adozione di misure opportune per la riduzione del rischio a livello accettabile. La consultazione preventiva è assoggettata al rispetto delle disposizioni di cui all'art. 36.

4. Ai sensi degli artt. 35, par. 4, e 57, par. 1, lett. k), del GDPR, fermo restando quanto indicato

nelle “Linee guida in materia di valutazione d'impatto sulla protezione dei dati”, il Garante per la protezione dei dati personali ha individuato, con Provvedimento n. 467 dell’1 ottobre 2018, l’ “*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell’art. 35, comma 4, del Regolamento (UE) n. 2016/679”,* soggetti al meccanismo di coerenza, da sottoporre a valutazione d’impatto. L’elenco è il seguente:

1.Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad “aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

2.Trattamenti automatizzati finalizzati ad assumere decisioni che producono “*effetti giuridici*” oppure che incidono “*in modo analogo significativamente*” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere;

3.Trattamenti che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc;

4.Trattamenti su larga scala di dati aventi carattere estremamente personale così come disciplinati dalle “Linee guida in materia di valutazione d'impatto sulla protezione dei dati” adottate dal Gruppo di Lavoro Art. 29; in particolare si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata o che incidono sull’esercizio di un diritto fondamentale oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato, quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti;

5.Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti, così come dettagliato nelle Linee guida sopra riportate;

6.Trattamenti non occasionali di dati relativi a soggetti vulnerabili, quali ad esempio minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo;

7.Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo, quali ad esempio IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad esempio il *wi-fitracking*, ogni qualvolta ricorra anche almeno un altro dei criteri individuati nelle Linee guida sopra riportate;

8.Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;

9.Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento, quali ad esempio il *mobile payment*;

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 del GDPR oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse;

11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento;

12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Tale elenco è riferito esclusivamente a tipologie di trattamento soggette al meccanismo di coerenza e non è esaustivo, restando fermo quindi l'obbligo di adottare una D.P.I.A. laddove ricorrano due o più dei criteri individuati in materia dalle Linee guida del Gruppo di Lavoro Art. 29 e che in taluni casi "un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno dei predetti criteri richieda una valutazione d'impatto sulla protezione dei dati".

5. Il Titolare:

- garantisce l'effettuazione della D.P.I.A. ed è responsabile della stessa;
- può affidare la conduzione materiale della D.P.I.A. ad un altro soggetto, interno o esterno all'Ente;

- deve consultarsi con il R.P.D. anche per assumere la decisione di effettuare o meno la D.P.I.A. Tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della D.P.I.A;
- può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati;
- deve procedere alla consultazione preventiva del Garante per il trattamento dei dati personali, prima di procedere al trattamento, se le risultanze della D.P.I.A. condotta indicano l'esistenza di un rischio residuale elevato, che non è stato attuato neppure a fronte dell'adozione di misure tecniche ed organizzative adeguate;
- consulta il Garante Privacy nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

6. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della D.P.I.A. fornendo ogni informazione necessaria.

7. Il Responsabile della protezione dati (R.P.D.-D.P.O.) monitora lo svolgimento della D.P.I.A. e può proporre lo svolgimento di una D.P.I.A. in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

8. E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una dichiarazione relativa all'effettuazione della D.P.I.A..

Articolo 12 - Violazione dei dati personali

1. La violazione dei dati personali è definita coma la *"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati"* dal Titolare o dal Responsabile del trattamento (art. 4, n. 12, Regolamento (UE) 2016/679). Al riguardo si definiscono le seguenti tipologie:

- *distruzione:* si ha "distruzione" di dati personali quando non esistono più o non esistono più in una forma che possa essere di qualsiasi utilità per il Titolare;
- *perdita:* il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento ha perso il controllo o l'accesso oppure non ha più il possesso
- "danno": si verifica quando i dati personali sono stati alterati, corrotti o non sono più completi;
- *trattamento non autorizzato o illecito:* il "trattamento non autorizzato o illecito" può includere la divulgazione di dati personali a (o accesso da parte di) destinatari che non sono

autorizzati a ricevere (o accedere a) i dati, o qualsiasi forma di trattamento che viola il Regolamento.

2. In caso di violazione dei dati personali, il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, ha l'obbligo di notificare la violazione (c.d. *"data breach"*) al 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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo (art. 33 GDPR).

3.Il Responsabile del trattamento in caso di violazione dei dati personali è obbligato ad informare il Titolare, senza ingiustificato ritardo ed in ogni caso entro 24 ore dal momento in cui ne è venuto a conoscenza (cd. *"data breach"*), per consentire al Titolare la notificazione all'Autorità di Controllo entro i termini previsti dall'art. 33, comma 1, del Regolamento (UE) 2016/679, ovvero, entro 72 ore dal momento in cui ne è venuto a conoscenza.

4. La notifica deve almeno:

a) descrivere la 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 registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

6. Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

7. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al GDPR, sono i seguenti (*a titolo non esaustivo*):

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

giudiziari).

8. Se il Titolare ritiene che il rischio per i diritti e le libertà delle persone fisiche ovvero degli interessati conseguente alla violazione rilevata è elevato, allora deve informare, -salvo i casi riportati al comma 8 del presente articolo-, questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. La comunicazione agli interessati deve contenere almeno le informazioni e le misure di cui al paragrafo 4, lettere b), c) e d), del presente articolo, ai sensi dell'art. 34 del GDPR.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi;
- comportare rischi imminenti e con un'elevata probabilità di accadimento, quali ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito;
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni, quali ad esempio utenti deboli, minori, soggetti indagati.

9. Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

10. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al precedente comma 8 è soddisfatta.

11. Il Titolare deve opportunamente e comunque documentare le violazioni di dati personali subite, anche se non comunicate all'autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante per la protezione dei dati personali al fine di verificare il rispetto delle disposizioni del Regolamento (UE) 2016/679.

12. Tali disposizioni sono ulteriormente analizzate nelle Linee Guida adottate dal Gruppo di Lavoro Articolo 29 in data 3 ottobre 2017 ed approvate nella versione emendata il 6 febbraio 2018.

13. Il Titolare del trattamento adotterà un Registro dei casi di *data breach*, in cui verranno annotati i casi di violazione effettivamente occorsi e le minacce potenziali, e ciò al fine di identificare il tipo e la natura delle violazioni più ricorrenti.

14. Il tracciamento dei casi di violazione dei dati personali verrà effettuato allo scopo di:

- individuare e tenere sotto controllo i fattori di rischio, ossia i fattori che determinano con più frequenza una violazione dei dati personali;
- misurare l'efficacia delle *policy* e delle procedure adottate;
- elaborare un piano di conformità che fissi gli obiettivi da raggiungere per essere *"compliant"* rispetto a leggi, *best practices*, e che aiuti a dimostrare la conformità in sede di audit di verifica/ispezioni/test;

Per gestire e risolvere i casi di *data breach* l'Ente si avvale principalmente della propria struttura, secondo gli ambiti di propria competenza, potendo ricorrere a soluzioni esterne nei casi di particolare complessità e qualora risulti necessario acquisire professionalità non in dotazione all'Ente stesso.

Articolo 13 - Rinvio

1. Per tutto quanto non espressamente previsto e disciplinato con il presente regolamento, si applicano le disposizioni del Regolamento europeo, leggi e regolamenti vigenti e le Linee guida approvate dal Gruppo Art. 29 per la protezione dei dati personali.

PARTE II
REGOLAMENTO PER L'INSTALLAZIONE E L'UTILIZZO DI IMPIANTI DI VIDEOSORVEGLIANZA

CAPO I - PRINCIPI GENERALI

Articolo 1 - Oggetto

1. Il presente regolamento definisce le linee generali e tecniche per l'attuazione di un sistema di sicurezza integrata in attuazione di quanto stabilito dall'art. 2 del decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla Legge 18 aprile 2017, n. 48, recante *"Disposizioni urgenti in materia di sicurezza delle città"*. Si tratta di un sistema unitario e integrato di sicurezza per il benessere della comunità territoriale del Comune di Cesena che, attraverso un'attenta programmazione urbana, mira a ridurre le opportunità di commettere reati unitamente alle misure volte a sostenere la partecipazione dei cittadini al miglioramento complessivo delle condizioni sociali e abitative, nel rispetto delle diverse competenze delle forze di Polizia Locale e dello Stato.
2. In tal senso, il Comune di Cesena e la Prefettura-UTG di Forlì-Cesena hanno stipulato, in data 23 febbraio 2017, un *"Protocollo d'Intesa per la gestione del sistema di videosorveglianza cittadino"*. In attuazione del suddetto protocollo la Polizia Locale gestirà gli impianti per prevalenti esigenze di sicurezza urbana, mentre Carabinieri e Polizia di Stato li utilizzeranno per esigenze di sicurezza e ordine pubblico.
3. Il presente regolamento è, quindi, finalizzato alla tutela dell'incolumità pubblica, della sicurezza urbana e ambientale attraverso la prevenzione dei reati, il controllo delle aree e delle attività soggette a rischio; garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di impianti di videosorveglianza integrata nel territorio urbano, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza ed all'identità personale.

Art. 2 - Definizioni

1. Ai fini del presente regolamento s'intende:
   a) per **"banca dati"**, il complesso di dati personali formatosi mediante riprese audiovisive che, in relazione ai luoghi di installazione delle videocamere, riguardano prevalentemente i soggetti ed i veicoli che transitano nell'area interessata;
   b) per **"impianto di videosorveglianza"**, l'impianto costituito da una rete di telecamere dislocate nel territorio comunale, dirette a riprendere e registrare immagini e suoni, utilizzate per le finalità indicate nel presente regolamento;
   c) per **"trattamento"**, tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'estrazione, l'elaborazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione

mediante trasmissione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distribuzione di dati;

d) per **"dato personale"**, qualsiasi informazione relativa a persona fisica, identificata o identificabile, rilevata attraverso l'impianto di videosorveglianza o i dispositivi mobili;
e) per **"titolare del trattamento"**, il Comune di Cesena, in persona del Sindaco p.t., la Prefettura-UTG Provincia di Forlì-Cesena, in persona del Prefetto p.t.;
f) per **"contitolare del trattamento"**, due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali;
g) per **"responsabile del trattamento"**, il Settore Polizia Municipale rappresentato organicamente dal Comandante p.t., il Questore e il Comandante Provinciale dell'Arma dei Carabinieri ovvero la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
h) per **"incaricati del trattamento"**, le persone fisiche autorizzate al trattamento dei dati personali da parte del Titolare o del Responsabile del trattamento;
i) per **"interessato"**, la persona fisica, la persona giuridica, l'ente o associazione cui si riferiscono i dati personali;
j) per **"comunicazione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
k) per **"diffusione"**, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
l) per **"dato anonimo"**, il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
m) per **"blocco"**, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
n) per **"Codice"**, il Decreto Legislativo 30 giugno 2003 n. 196 recante il "Codice in materia di protezione dei dati personali", modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
o) per **"GDPR",** General Data Protection Regulation, ovvero il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (regolamento generale sulla protezione dei dati).

Articolo 3 - Ambito di applicazione

1. Il presente regolamento disciplina il trattamento dei dati personali, realizzato dal Comune di Cesena, in persona del Sindaco p.t., mediante gli impianti di videosorveglianza in luoghi pubblici, attivati nel territorio del Comune di Cesena.
2. L'Utilizzo dei sistemi della videosorveglianza e dei dati da essi raccolti viene attuato nel rispetto dei principi di:

- **liceità**, quale rispetto delle normative vigenti, sia per gli organi pubblici che privati;

- **proporzionalità**, con sistemi attuati e collocati a seguito di attenta valutazione. In applicazione al principio di proporzionalità, pur essendo consentiti margini di libertà nella valutazione da parte del titolare del trattamento, non sono ammesse scelte del tutto discrezionali e insindacabili. Va in generale evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli o per le quali non ricorre un'effettiva esigenza di deterrenza. Il trattamento dei dati è pertinente e non eccedente rispetto alle finalità perseguite;
- **finalità,** attuando il trattamento dei dati solo per scopi determinati ed espliciti esclusivamente per lo svolgimento delle proprie funzioni istituzionali;
- **necessità**, con esclusione di uso superfluo della videosorveglianza. Tale principio prevede che i sistemi informativi e i programmi informatici vengano configurati riducendo al minimo l'utilizzazione dei dati personali; pertanto andranno evitati eccessi e ridondanze nei sistemi di videosorveglianza;
- **economicità, efficacia ed efficienza** costituiscono corollario del canone di buon andamento dell'azione amministrativa (consacrato dall'art. 97 Cost.), che impone alla pubblica amministrazione il conseguimento degli obiettivi legislativamente statuiti ovvero realizzati attraverso il sistema di videosorveglianza integrata con i privati, con il minor dispendio di mezzi e di strumenti.

3. La dislocazione degli impianti di videosorveglianza e l'utilizzo degli stessi verrà strutturata sulla base di specifico progetto operativo da sottoporre a preventiva "Valutazione d'impatto sulla protezione dei dati" (DPIA) ai sensi di quanto previsto dagli articoli 35 e ss. del Regolamento (UE) 2016/679, da assumersi con separato atto, anche tenendo conto delle priorità che verranno individuate in termini di sicurezza, presidio e controllo del territorio.

4. Tali impianti:

a) riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone fisiche ed i mezzi di trasporto che transitano nell'area interessata;
b) consentono unicamente riprese video e audio-video per i dispositivi mobili;
c) sono installati in corrispondenza dei luoghi indicati in sede di progetto attuativo, come previsto dal precedente comma.

5. Sono attivabili impianti di fotosorveglianza e videosorveglianza mobili, posizionabili in aree del territorio comunale individuate dal Corpo di Polizia Locale oppure montate su veicoli di servizio e utilizzabili per le finalità indicate nel presente regolamento.

6. L'impianto di videosorveglianza potrà essere composto da:

a) rete di telecamere fisse e sistemi di elaborazione collegati in fibra ottica e dedicati alla sorveglianza di alcuni siti del Comune;
b) rete di telecamere, per la lettura e riconoscimento targhe veicoli, poste sulle principali arterie di entrata ed uscita dal territorio comunale;
c) apparecchiature di rilevazione della targa dei veicoli in transito, apposte lungo i varchi di accesso alla ZTL cittadina, ai fini dell'accertamento delle violazioni al Codice della Strada. La disciplina relativa al trattamento dati di cui al presente regolamento si applica a tali

apparecchi, in quanto e nei limiti in cui consentono la ripresa delle immagini e la registrazione dei dati alfanumerici contenuti nelle targhe veicolari;

d) telecamere mobili per lettura e riconoscimento targhe;
e) telecamere mobili per vigilanza sui rifiuti e finalità di polizia giudiziaria (P.G.);
f) telecamere mobili, per la registrazione audio e video degli interventi, denominate *body cam* (telecamere applicate sulle divise degli agenti) e *dash cam* (telecamere a bordo veicoli di servizio) in dotazione alla Polizia Locale e utilizzate per i servizi a maggior rischio operativo, per finalità di P.G e allo scopo di tutelare sia i soggetti coinvolti nelle operazioni di polizia che gli stessi agenti.

Le telecamere indicate come 'lettura targhe' sono apparati in grado di rilevare le targhe dei veicoli in transito e consentono il riconoscimento delle targhe con un sistema di rilevamento automatico dei caratteri (OCR).

7. In particolare, il presente regolamento:
- definisce gli impianti di videosorveglianza fissi, mobili e di lettura targhe, di proprietà del Comune di Cesena o da esso gestiti, che potranno essere installati;
- disciplina le principali caratteristiche e le modalità di utilizzo degli impianti di videosorveglianza;
- disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza.

8. Il sistema di videosorveglianza del Comune di Cesena è integrato con le apparecchiature di rilevazione della targa dei veicoli in transito, apposte lungo i varchi di accesso alla ZTL cittadina, al fine del controllo del rispetto degli accessi. La disciplina relativa al trattamento dati di cui al presente regolamento si applica a tali apparecchi, in quanto e nei limiti in cui consentono la ripresa delle immagini e la registrazione dei dati alfanumerici contenuti nelle targhe veicolari.

9. I sistemi di videosorveglianza già in essere sul territorio e quelle di futura installazione si potranno concentrare in diverse centrali di controllo, di cui al richiamato *"Protocollo d'intesa tra Prefettura Ufficio territoriale del Governo di Forlì-Cesena e Comune di Cesena, per la gestione del sistema di videosorveglianza cittadino"*. La centrale di comando principale è la Centrale Operativa del Corpo di Polizia Locale sita in Via Natale Dell'Amore n. 19 a Cesena.

10. L'utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada, in considerazione della peculiarità dei fini istituzionali perseguiti, non è assoggettato alla disciplina di cui al presente regolamento, ma alle disposizioni dettate dal Garante della privacy nel decalogo dell'8 aprile 2010, al paragrafo 5.3, ed al provvedimento n. 467 dell'11 ottobre 2018 (obbligatorietà della DPIA), nonché dalla specifica normativa di settore.

Articolo 4 - Finalità e trattamento dei dati personali acquisiti e gestiti tramite gli impianti di videosorveglianza

1. Il trattamento dei dati personali è effettuato tramite gli impianti di videosorveglianza.

2. Le finalità di utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono conformi alle funzioni istituzionali demandate al Comune di Cesena dalla Legge quadro 7 marzo

1986, n. 65 sull'Ordinamento della Polizia Municipale, dalla Legge Regionale 4 dicembre 2003, n. 24, recante *"Disciplina della polizia amministrativa locale e promozione di un sistema integrato di sicurezza"* e successive modifiche e integrazioni (da ultimo la Legge Regionale 30 luglio 2018, n. 13), allo Statuto e dai regolamenti comunali, nonché dal Decreto Legge 20 febbraio 2017, n. 14, convertito in Legge 18 aprile 2017, n. 48 *"Disposizioni urgenti in materia di sicurezza delle città"*. In particolare, l'uso di impianti di videosorveglianza è strumento per l'attuazione di un sistema integrato di politiche per la sicurezza urbana, di cui alle fonti normative sopra citate.

3. L'utilizzo degli impianti di videosorveglianza è finalizzato a:

a) attivazione di uno strumento attivo di Protezione Civile sul territorio comunale;
b) monitoraggio del traffico in tempo reale, al fine di consentire il pronto intervento della Polizia Locale;
c) comunicazione agli utenti della strada di ogni notizia utile sulla viabilità;
d) rilevazione di dati anonimi per l'analisi dei flussi di traffico e per la predisposizione dei piani comunali del traffico;
e) prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce e la prevenzione delle stesse, in particolare:
   - prevenzione di eventuali atti di vandalismo o di danneggiamento agli immobili pubblici ed in particolare al patrimonio comunale e di disturbo alla quiete pubblica;
   - prevenzione e repressione di atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del Decreto-Legge n. 14/2017, coordinato con la Legge n. 48/2017, delle attribuzioni del Sindaco in qualità di Autorità Locale di cui all'art. 50 e di Ufficiale di Governo di cui all'art. 54, comma 4 e 4-*bis* del D.Lgs. 18 agosto 2000, n. 267;
   - prevenzione e repressione degli illeciti, di natura penale o amministrativa, in particolare legati a fenomeni di degrado urbano e abbandono di rifiuti, con controlli volti ad accertare e sanzionare le violazioni delle norme in materia ambientale e delle norme contenute nel Codice di Convivenza Civile, nei regolamenti locali in genere e nelle ordinanze sindacali;
f) controllo delle aree specifiche del territorio comunale;
g) monitoraggio del sistema di gestione centralizzata degli impianti semaforici.

4. A presidio di particolari obiettivi sensibili, così come definiti nel richiamato progetto operativo di cui al precedente articolo 3, comma 3, potranno attivarsi sistemi di telecamere che entrano in funzione solo in caso di intrusione nell'area pertinenziale di questi, rilevando in automatico comportamenti o eventi anomali, provvedendo alla segnalazione e registrazione, e, se del caso, azionando un sistema di illuminatori ottici o allarme acustico. L'utilizzo di tali sistemi è subordinato alla preventiva esecuzione di "Valutazione d'impatto sulla protezione dei dati" (DPIA),

secondo quanto previsto dagli articoli 35 e ss. del Regolamento (UE) 2016/679.
5. Il sistema di videosorveglianza comporterà esclusivamente il trattamento dei dati personali rilevati mediante le riprese televisive e che, in relazione ai luoghi di installazione delle videocamere, interesserà i soggetti ed i mezzi di trasporto che si troveranno a transitare nell'area interessata.
6. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso del sistema di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione previo controllo da parte del Garante o specifiche richieste dell'autorità giudiziaria.
7. L'uso dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate all'apposita normativa vigente in materia di "privacy".

CAPO II - SOGGETTI DEL TRATTAMENTO

Articolo 5 - Titolare e Contitolare del trattamento

1. Il Comune di Cesena, in persona del Sindaco p.t. e la Prefettura-UTG Provincia di Forlì-Cesena, in persona del Prefetto p.t., sono Titolari e Contitolari del trattamento dei dati personali acquisiti mediante utilizzo degli impianti di videosorveglianza di cui al presente regolamento. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare e il Contitolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento (UE) 2016/679 e al D.Lgs. 30 giugno 2003, n. 196, modificato dal D.Lgs. 10 agosto 2018, n. 101.
2. In conformità a quanto stabilito dagli articoli 33 e 34 del Regolamento (UE) 2016/679, in caso di violazione dei dati personali e ricorrendo i presupposti di legge, il Titolare o il Contitolare del trattamento notificano la violazione all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sono venuti a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare o il Contitolare del trattamento comunicano la violazione all'interessato senza ingiustificato ritardo. Non è richiesta la comunicazione all'interessato se è soddisfatta una delle condizioni di cui paragrafo 3 del citato articolo 34.
3. Il Titolare del trattamento ha designato il Responsabile del trattamento e il Responsabile della protezione dei dati personali (RPD-DPO).
4. Il Titolare del trattamento, assoggettato al rispetto delle disposizioni del Regolamento (UE) 2016/679 in merito alla "Valutazione d'impatto sulla protezione dei dati" (DPIA), ai sensi dell'articolo 35 e ss. del Regolamento (UE) 2016/679, potrà richiedere al Responsabile della

protezione dei dati (RPD-DPO) un suo parere nonché di sorvegliare lo svolgimento della DPIA. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie e la sorveglianza sistematica su larga scala, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, consultando la competente Autorità di controllo.

5. I soggetti coinvolti (Comune di Cesena, Prefettura e Forze di Polizia), tratteranno i dati personali in qualità di Titolari o Contitolari del trattamento, (*ex* art. 26 GDPR 2016/679 e art. 17 D.Lgs 18 maggio 2018, n. 51), secondo quanto stabilito dalle disposizioni normative e regolamentari in materia. All'uopo verranno stipulati accordi interni per stabilire le rispettive responsabilità.

Articolo 6 - Responsabile del trattamento dei dati personali

1. I Responsabili del trattamento dei dati personali rilevati dal sistema di videosorveglianza sono:
   a) il Settore Polizia Municipale del Comune di Cesena, rappresentato organicamente dal Comandante p.t.;
   b) il Questore e il Comandante Provinciale della Provincia Forlì-Cesena.

2. Il Responsabile del trattamento, che tratta i dati personali per conto del Titolare del trattamento, deve rispettare pienamente quanto previsto dalle leggi vigenti e dalle disposizioni del presente regolamento in materia di trattamento e sicurezza dei dati personali.

3. La gestione tecnica dell'impianto e la manutenzione sono affidati a soggetti esterni specializzati, all'uopo appositamente individuati e designati dal Titolare del trattamento, assoggettati al rispetto della normativa vigente in materia di trattamento dei dati personali.

Articolo 7 - Persone autorizzate al trattamento dei dati personali

1. Il Comandante del Corpo di Polizia Municipale di Cesena, il Questore e il Comandante Provinciale della Provincia Forlì-Cesena, nei casi previsti dalla legge, nominano gli incaricati (persone autorizzate al trattamento dei dati) mediante atto scritto, in numero sufficiente a garantire il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento.

2. Le persone autorizzate effettuano il trattamento attenendosi scrupolosamente alle istruzioni impartite dal Titolare, dal Contitolare o dal Responsabile del trattamento dei dati personali.

3. Nell'ambito delle persone autorizzate al trattamento, sono altresì designati, con atto di nomina, i soggetti ai quali sono affidate la custodia e la conservazione delle chiavi di accesso ai locali delle centrali di controllo e delle chiavi dei locali nonché degli armadi nei quali sono custoditi i supporti contenenti le registrazioni.

CAPO III - TRATTAMENTO DEI DATI PERSONALI

Articolo 8 - Modalità di raccolta, trattamento e conservazione dei dati personali

1. I dati personali oggetto di trattamento sono:
   a) trattati in modo lecito e secondo i principi espressi nel precedente articolo 3;
   b) raccolti e trattati per le finalità di cui al precedente art. 4 e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;
   c) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dal successivo comma 3. Trascorso tale periodo i dati dovranno essere cancellati nel rispetto di quanto stabilito dal successivo comma 3.

2. I dati personali sono ripresi attraverso le telecamere degli impianti di telecontrollo e di videosorveglianza, installati in corrispondenza di qualsiasi posizione del territorio urbano ritenuto di interesse per le finalità istituzionali di cui all'art. 4, comma 3**.**

3. Sulla base delle disposizioni normative vigenti, il termine massimo di durata della conservazione dei dati 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. La conservazione dei dati personali per un periodo di tempo superiore a quello indicato è ammessa esclusivamente su specifica richiesta dell'Autorità Giudiziaria o di Polizia Giudiziaria in relazione ad un'attività investigativa in corso. In tali casi dovrà essere informato il Comandante della Polizia Locale di Cesena, che darà esplicita autorizzazione ad operare per tale fine.

4. Fuori delle ipotesi espressamente previste dal comma 3 del presente articolo, la conservazione dei dati personali per un tempo eccedente i sette giorni è subordinata ad una verifica preliminare del Garante per la protezione dei dati personali. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità 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.

5. Il sistema di conservazione delle immagini, se automatizzato, dovrà essere programmato in modo da operare, al momento prefissato, l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. 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.

Articolo 9 - Obblighi degli operatori

1. L'utilizzo delle impostazioni generali di videoregistrazione (area di ripresa, brandeggio della telecamera, zoom, ecc.) da parte degli operatori e degli incaricati/soggetti autorizzati al trattamento dovrà essere conforme ai principi del presente regolamento e delle norme di riferimento.
2. L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolga nei luoghi pubblici mentre esso non è ammesso nelle proprietà private.
3. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità.
4. La mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.

Articolo 10 - Accertamenti di illeciti e indagini dell'Autorità Giudiziaria e/o di Polizia

1. Ove dovessero essere rilevate immagini di fatti relativi a ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, l'incaricato od il Responsabile della videosorveglianza provvederà a darne immediata comunicazione agli organi competenti. In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa di cui al precedente articolo 8, l'incaricato procederà alla registrazione delle stesse.
2. Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di Polizia e l'Autorità Giudiziaria.
3. Tutte le strumentazioni di videosorveglianza potranno essere utilizzate anche in relazione ad indagini disposte dall'Autorità Giudiziaria, di organi di Polizia o di Polizia Locale. Nel caso in cui gli organi di Polizia, nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate che sono contenute nelle riprese effettuate, possono farne richiesta scritta e motivata indirizzata al Titolare o al Responsabile del trattamento dei dati.

Articolo 11 - Informazioni rese al momento della raccolta

1. Il Comune di Cesena, in ottemperanza a quanto disposto dalla deliberazione 8 aprile 2010 relativa al provvedimento del Garante in materia di videosorveglianza, e del Codice, previa esecuzione della DPIA di cui all'art. 35 GDPR 2016/679, si obbliga ad affiggere un'adeguata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere, su cui è riportata la seguente dicitura: *"Area videosorvegliata - La registrazione è effettuata dalla Polizia Locale per fini di sicurezza urbana"*.
2. Fermo quanto previsto dal comma 1 del presente articolo, il Comune di Cesena rende noto agli interessati il funzionamento degli impianti di videosorveglianza tramite le seguenti forme semplificate di informativa:

a) pubblicazione sul sito internet istituzionale di planimetrie e di altra documentazione relative alle zone videosorvegliate;
b) cartelli di cui all'informazione minima prevista installati nei varchi d'accesso alla città e, in alcuni specifici casi, in prossimità degli impianti.

3. Può essere omessa l'installazione di cartellonistica contenente l'informativa di cui sopra nei casi di utilizzo di telecamere a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati.

4. Fermo quanto previsto dal comma 1 del presente articolo, il Comune di Cesena rende noto agli interessati il funzionamento degli impianti di videosorveglianza, installati all'interno di edifici comunali, tramite posizionamento di cartelli contenenti l'informativa. Gli impianti di videosorveglianza installati all'interno di edifici comunali non sono utilizzati per effettuare controlli a distanza dell'attività lavorativa dei dipendenti dell'Amministrazione comunale, ma esclusivamente per le finalità di cui al presente regolamento.

5. Gli interessati dovranno 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).

Articolo 12 - Diritti dell'interessato

1. Il Titolare del trattamento mette a disposizione dell'interessato, anche sul proprio sito internet, le seguenti informazioni:

a) l'identità e i dati di contatto del Titolare/Contitolare del trattamento;
b) i dati di contatto del Responsabile della protezione dei dati;
c) le finalità del trattamento cui sono destinati i dati personali;
d) la sussistenza del diritto di proporre reclamo al Garante e i relativi dati di contatto;
e) la sussistenza del diritto di chiedere al Titolare o al Contitolare del trattamento, ove ricorrano le ipotesi di legge, l'accesso ai dati o la cancellazione dei dati personali e la limitazione del trattamento dei dati personali che lo riguardano;
f) l'informazione che l'interessato potrà esercitare i propri diritti nei confronti di e contro ciascun Titolare del Trattamento e il punto di contatto per gli interessati.

2. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza e ove ricorrano i presupposti di legge, ha diritto:

a) di conoscere l'esistenza di trattamenti dei dati che possono riguardarlo;
b) di essere informato sugli estremi identificativi del Titolare e del Responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
c) di ottenere, a cura del Responsabile del trattamento, senza ritardo dalla data di ricezione della richiesta:
   - la conferma dell'esistenza o meno di dati personali che lo riguardano e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento; la richiesta non può essere inoltrata dallo

stesso soggetto se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi;

- la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti e successivamente trattati;
- di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

3. 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 dì protezione.

4. Nell'esercizio dei diritti di cui al comma 2, 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.

5. Le istanze di cui al presente articolo possono essere trasmesse al Titolare o al Responsabile anche mediante lettera raccomandata, PEC (posta elettronica certificata) o SERC (Servizio Elettronico di Recapito Certificato), che dovrà provvedere in merito entro e non oltre trenta giorni.

6. Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice e alle leggi vigenti in materia, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.

7. 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 solo nei limiti previsti dal Codice e dalle leggi vigenti in materia, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

8. 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.

9. Nel caso di esito negativo alle istanze 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.

CAPO IV - SISTEMI DI VIDEOSORVEGLIANZA

Articolo 13 - Sistemi integrati di videosorveglianza

1. Nell'ambito dei trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

a) gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento; in tale ipotesi, i singoli titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;

b) collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'art. 28 GDPR (UE) 2016/679 da parte di ogni singolo Titolare o, previa intesa, da uno dei due Contitolari, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza;
c) sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia.

2. La dislocazione degli impianti di videosorveglianza e l'utilizzo degli stessi verrà strutturata sulla base di specifico progetto operativo da sottoporre a preventiva "Valutazione d'impatto sulla protezione dei dati" (DPIA) ai sensi di quanto previsto dagli articoli 35 e ss. del Regolamento (UE) 2016/679, da assumersi con separato atto, anche tenendo conto delle priorità che verranno individuate in termini di sicurezza, presidio e controllo del territorio.

Articolo 14 - Utilizzo di particolari dispositivi mobili

1. Gli impianti di videosorveglianza mobile verranno utilizzati per la tutela del patrimonio comunale e delle aree pubbliche, quale ausilio per le attività di controllo volte ad accertare l'abbandono dei rifiuti di qualsiasi natura, nonché a monitorare il rispetto delle disposizioni in materia di raccolta dei rifiuti, soltanto quando le altre misure di sicurezza e di tutela siano ponderatamente valutate insufficienti o inattuabili.

2. Gli operatori di Polizia Locale nell'espletamento delle proprie funzioni, potranno fare uso anche di dispositivi di audio-video ripresa mediante l'utilizzo d'idonea strumentazione tecnica in dotazione. Per specifiche finalità gli operatori di Polizia Locale possono essere dotati di sistemi di microtelecamere per l'eventuale ripresa di situazioni di criticità per la sicurezza.

3. Spetta all'Ufficiale di Polizia Giudiziaria, che impiega direttamente il personale operativo, impartire l'ordine di attivazione dei dispositivi in relazione all'evolversi degli scenari di sicurezza e ordine pubblico che facciano presupporre criticità. Lo stesso ne disporrà la disattivazione. Al termine del servizio gli operatori interessati, previa compilazione di un foglio di consegna, affideranno tutta la documentazione video realizzata all'Ufficiale responsabile.

4. Il trattamento dei dati personali effettuati con simili sistemi di ripresa devono rispettare i principi del Codice ed in particolare i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati.

Articolo 15 - Sistemi di videosorveglianza messi a disposizione da soggetti terzi

1. I privati e/o soggetti terzi, singoli o associati possono partecipare all'estensione e all'implementazione del sistema di videosorveglianza cittadino mediante l'acquisto diretto e la conseguente cessione al Comune di Cesena della strumentazione utile ad integrare l'impianto

esistente anche sulla base di specifiche intese assunte o da assumersi con le associazioni di categoria e di rappresentanza sindacale.
2. A tal fine presenteranno apposita istanza per aderire alla rete integrata di videosorveglianza allegando planimetria e relazione tecnica, documentazione, che visionata e avvallata dal Comando di Polizia Locale, tramite il Sindaco sarà portata all'attenzione del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica. La collocazione, l'uso e/o la visione degli apparecchi forniti dai soggetti di cui al comma 1, pur inglobando e/o interessando accessi di interesse privato, dovranno comunque avere una preminente rilevanza pubblica (vincolo d'immagine su aree pubbliche, pur inglobando accessi privati), confermata dopo l'esame dell'istanza dal Comando di Polizia Locale che curerà altresì l'individuazione delle caratteristiche tecniche minime delle strumentazioni offerte di cui al comma precedente.
3. La strumentazione di videosorveglianza dovrà essere fornita, installata e l'eventuale collegamento alla centrale di gestione dell'impianto cittadino sarà a cura e spese dei soggetti privati.
4. La manutenzione ordinaria e straordinaria delle telecamere, ivi compresa la sostituzione dovuta a danni derivanti da terzi, da eventi meteorologici, da atti vandalici o per la vetustà dell'apparecchio, sarà a carico dei soggetti privati.
5. I privati e/o soggetti terzi, singoli o associati non svolgono e non potranno mai svolgere alcuna attività di "trattamento dei dati".

Articolo 16 - Censimento degli impianti di videosorveglianza attivi nel territorio comunale

1. I Titolari di impianti di videosorveglianza già attivi nel territorio comunale sono obbligati a comunicare al Comune di Cesena entro 90 giorni dalla data in cui entra in vigore il presente regolamento ovvero 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.

2. Tale comunicazione consentirà di censire tutti gli impianti di videosorveglianza presenti nel territorio comunale, con loro geolocalizzazione e l'identificazione dei titolari e responsabili del trattamento. La mappatura, con immediata identificazione e reperibilità di tutti gli impianti di videosorveglianza presenti nel territorio comunale, potrà rafforzare la capacità di indagine di Magistratura e Forze dell'Ordine, non solo nell'attività di prevenzione ma, soprattutto, nella più efficace possibilità di acquisire informazioni utili al perseguimento di un fatto criminoso così da avere, nella sua immediatezza, la capacità di sapere quali registrazioni sarebbe utile verificare, potendo subito acquisire le immagini, le quali, diversamente, sarebbero automaticamente cancellate e perse.
3. La comunicazione dei predetti dati sarà effettuata con modalità semplificate utilizzando anche apposita modulistica ovvero apposito *form* per l'inserimento nella sezione dedicata predisposta su

un sito internet comunale, visionabile esclusivamente dalla Polizia Locale e dalle Forze di Polizia Statali.
4. Con le stesse modalità e nello stesso termine di 60 giorni, il titolare dell'impianto dovrà comunicare eventuali variazione dei dati precedentemente comunicati.
5. Sono esclusi dall'obbligo di comunicazione gli impianti attivi all'interno di aree private. 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.
6. I dati raccolti saranno trattati, nel rispetto della disciplina dettata dalla vigente normativa di settore, nella esclusiva disponibilità di Magistratura, Autorità di Pubblica Sicurezza e per le attività di indagine di polizia giudiziaria, secondo modalità operative puntualmente concordate con il responsabile del loro trattamento.

Articolo 17 - Abbandono dei rifiuti

1. In applicazione dei richiamati principi di necessità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta consentito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali generici e/o di materiali o sostanze pericolose.
2. L'utilizzo di sistemi di videosorveglianza è lecito nei casi in cui s'intenda monitorare il rispetto delle disposizioni concernenti tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente. Nello specifico, l'utilizzo della videosorveglianza da parte della Polizia Locale, in qualità di organo di polizia amministrativa, per sanzionare coloro che lasciano rifiuti di ogni genere lungo i margini della strada, fuori dai cassonetti o dalle apposite isole ecologiche, è stato espressamente previsto nel Provvedimento dell'8 aprile 2010 al punto 5.2., che consente di accertare le violazioni ai sensi dell'articolo 13 della Legge 24 novembre 1981, n. 689 e successive modifiche.
3. Il Comune si potrà avvalere anche di un impianto di videosorveglianza mobile per controllare particolari situazioni di degrado quali l'abbandono di rifiuti in prossimità di cassonetti, su aree pubbliche e nei parchi. I cittadini che transiteranno nelle aree sorvegliate saranno informati con cartelli della presenza delle telecamere.
4. Per particolari necessità o situazioni che richiedano l'utilizzo di attrezzature specializzate e personale esterno, il Titolare del trattamento può conferire la nomina di responsabile esterno a persone o società esterne con apposito atto che dovrà contenere disposizioni specifiche sul trattamento dei dati personali, ruoli, regole e modalità di trattamento.

CAPO V - SICUREZZA NEL TRATTAMENTO DEI DATI

Articolo 18 - Sicurezza dei dati

1. I dati raccolti mediante sistemi di videosorveglianza dovranno essere 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. Dovranno, quindi, essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa.

2. Le misure minime di sicurezza dovranno rispettare i seguenti principi:

a) i sistemi informativi e i programmi informatici destinati alla registrazione e alla conservazione dei dati personali raccolti attraverso sistemi di videosorveglianza sono configurati in conformità al criterio di necessità del trattamento dei dati personali;
b) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati/soggetti autorizzati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione complesse che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
c) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
d) le registrazioni delle operazioni debbono consentire di conoscere i motivi, la data e l'ora di tali operazioni e, se possibile, di identificare la persona che ha eseguito le operazioni e i destinatari;
e) 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;
f) tutte le operazioni di trattamento dati da parte degli operatori autorizzati deve avvenire tramite le postazioni informatiche (fisse o mobili) certificate e abilitate informaticamente;
g) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni potranno 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;
h) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;
i) sono adottate specifiche misure di sicurezza contro i rischi di accesso abusivo di cui all'articolo 615-*ter* del codice penale nei confronti degli apparati di ripresa digitale utilizzati ai fini della registrazione delle immagini qualora connessi a reti informatiche;
j) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che

ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless;

k) il Titolare o il Responsabile nella designazione dei soggetti incaricati/autorizzati al trattamento dei dati dovranno attenersi alle disposizioni del Regolamento (EU) 2016/679. Si dovrà trattare di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni, individuando altresì diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.). Viene stabilito che, in presenza di differenti competenze specificatamente attribuite ai singoli operatori, devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del 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;

l) ogni accesso ai dati sarà annotato in apposito registro su cui saranno indicati, a cura di un incaricato, identità della persona che accede ai dati, titolo d'accesso, orario di ingresso e uscita in caso di accesso all'archivio delle registrazioni. Questo registro cartaceo potrà essere sostituito da un registro elettronico (log), con pari caratteristiche di sicurezza ed attendibilità. Gli accessi ai file di log sono consentiti ai soli fini della verifica della liceità del trattamento, del controllo interno, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito del procedimento penale.

3. La trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless. Il Titolare o il Responsabile dovranno attenersi alle disposizioni del Regolamento (EU) 2016/679; si rinvia espressamente a quanto già indicato alla lettera "k" del presente articolo.

Articolo 19 - Registri delle attività di trattamento

1. I Titolari del trattamento tengono un registro di tutte le categorie di attività di trattamento sotto la propria responsabilità. Tale registro contiene le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, se previsti, di ogni contitolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) le categorie di destinatari;
d) una descrizione delle categorie di interessati e delle categorie di dati personali;
e) se previsto, il ricorso alla profilazione;

f) se previste, le categorie di trasferimenti di dati personali verso un Paese terzo o verso organizzazioni internazionali;
g) un'indicazione del titolo giuridico del trattamento cui sono destinati i dati personali, anche in caso di trasferimento;
h) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali;
i) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

2. I responsabili del trattamento tengono un registro di tutte le categorie di attività di trattamento svolte per conto di un titolare del trattamento, contenente le seguenti informazioni:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agiscono e, se esistente, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) eventuali trasferimenti di dati personali effettuati su istruzione del titolare del trattamento verso un Paese terzo o verso un'organizzazione internazionale;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

3. I registri di cui ai commi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico. Su richiesta, il Titolare del trattamento e il Responsabile del trattamento mettono tali registri a disposizione del Garante.

Articolo 20 - Cessazione del trattamento dei dati

1. In caso di cessazione per qualsivoglia motivo i dati personali saranno:

a) distrutti;
b) ceduti ad altro titolare purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
c) conservati per fini esclusivamente istituzionali dell'impianto attivato.

2. La cessione dei dati, in violazione di quanto previsto dal comma precedente lett. b) o di altre disposizioni di legge in materia di trattamento dei dati personali, è priva di effetti. Sono fatte salve le sanzioni previste dalla legge.

Articolo 21 - Comunicazione

1. La comunicazione dei dati personali da parte del Comune di Cesena a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento.

2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate, per iscritto, a compiere le operazioni del trattamento dal Titolare o dal Responsabile del trattamento e che operano sotto la loro diretta autorità.

3. E' vietata la comunicazione dei dati a qualsiasi soggetto privato, fatte salve le ipotesi di legge.

CAPO VI - DISPOSIZIONI FINALI

Articolo 22 - Disposizioni finali

1. L'aggiornamento dell'elenco degli impianti è demandato al Comandante del Settore Polizia Municipale, sulla base del progetto operativo di cui all'art. 3 del presente regolamento.
2. L'installazione e l'attivazione del sistema di videosorveglianza e l'utilizzo delle immagini sono subordinate alla preventiva esecuzione di Valutazione d'impatto (DPIA), secondo quanto previsto dagli articoli 35 e ss. del Regolamento (UE) 2016/679.

Articolo 23 - Norme di rinvio

1. Per quanto non espressamente disciplinato dal presente regolamento, si rinvia a quanto disposto da:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, in vigore dal 25 maggio 2018, relativo *"alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"*. L'art. 2, n. 2, lettera d), esclude l'applicazione del Regolamento europeo nei casi in cui il trattamento di dati personali venga effettuato dalle Autorità competenti per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse;
- D.Lgs. 30 giugno 2003, n. 196 *"Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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",* modificato dal D.Lgs. 10 agosto 2018, n. 101;
- Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa *"alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio"*;
- D.P.R. 15 gennaio 2018 n. 15 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 maggio 2018 n. 51 recante *"Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità*

competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio". L'art 1, n. 3, prevede che il decreto non si applica ai trattamenti di dati personali:

a) effettuati nello svolgimento di attività concernenti la sicurezza nazionale o rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea e per tutte le attività che non rientrano nell'ambito di applicazione del diritto dell'Unione europea;

b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione europea;

- Protocollo d'Intesa tra Prefettura Ufficio Territoriale del Governo di Forlì-Cesena e Comune di Cesena per la gestione del sistema di videosorveglianza cittadino del 23 febbraio 2017;
- 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;
- *"Linee generali delle politiche pubbliche per la promozione della sicurezza integrata, in attuazione dell'articolo 2 del Decreto-Legge 20 febbraio 2017 n. 14, convertito, con modificazioni, dalla Legge 18 aprile 2017 n. 48"*, approvate dalla Conferenza Unificata tra il Governo, Regioni e gli Enti locali, nella seduta del 24 gennaio 2018, con l'obiettivo di migliorare anche la qualità della vita nel territorio e la riqualificazione socio-culturale delle aree interessate;
- Direttive del Ministero dell'Interno n. 558/SICPART/421.2/70 del 2 marzo 2012 sui *"Sistemi di videosorveglianza in ambito comunale"* e n. 11001/110(23) del 30 aprile 2015, recante *"Nuove linee strategiche per il controllo coordinato del territorio"*;
- Provvedimenti dell'Autorità Garante per la protezione dei dati personali *"in materia di videosorveglianza"* dell'8 aprile 2010 (pubblicato in Gazzetta Ufficiale n. 99 del 29 aprile 2010) e n. 467 (allegato n. 1) dell'11 ottobre 2018 rubricato *"Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018"*, (pubblicato in Gazzetta Ufficiale, Serie Generale, n. 269 del 19 novembre 2018);
- Decreto-Legge 23 febbraio 2009, n. 11, convertito nella Legge 23 aprile 2009, n. 38 recante *"Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori"*;
- Decreto Ministero dell'Interno del 5 agosto 2008, recante disposizione in materia di *"Incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione"*;
- Legge Regionale Emilia-Romagna del 4 dicembre 2003 n. 24, recante *"Disciplina della polizia amministrativa locale e promozionale di un sistema integrato di sicurezza"* e successive modifiche.

Articolo 24 - Entrata in vigore

1. Il presente Regolamento entra in vigore dalla data di esecutività della deliberazione del Consiglio Comunale che lo approva.