COMUNE DI BAGNO DI ROMAGNA
MEDAGLIA D'ARGENTO AL VALORE CIVILE
Via Verdi, 4 - 47021 San Piero in Bagno (FC) Tel. 0543 900401 - Fax 0543 903032
protocollo@comune.bagnodiromagna.fc.it - www.comune.bagnodiromagna.fc.it
Gemellato con Moutiers (FR) Rapperswil (CH)

Codice per il trattamento dei dati personali e la videosorveglianza

Approvato con Deliberazione di Consiglio Comunale n. 8 del 15/04/2024
Modificato con Deliberazione di Consiglio Comunale n. 34 del 12/10/2026

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 pag. 3
Articolo 1 - Oggetto pag. 3
Articolo 2 - Finalità del trattamento pag. 3
Articolo 3 - Ambito di applicazione pag. 4
Articolo 4 - Definizioni pag. 4

CAPO II - SOGGETTI DEL TRATTAMENTO pag. 7
Articolo 5 - Titolare del trattamento pag. 7
Articolo 6 - Contitolari del trattamento pag. 8
Articolo 7 - Responsabile del trattamento pag. 9
Articolo 8 - Responsabile della protezione dati pag. 10

CAPO III - SICUREZZA DEL TRATTAMENTO pag. 13
Articolo 9 - Sicurezza del trattamento pag. 13
Articolo 10 - Registri delle attività di trattamento pag. 14
Articolo 11 - Valutazione d'impatto sulla protezione dei dati pag. 15
Articolo 12 - Violazione dei dati personali pag. 18
Articolo 13 - Rinvio pag. 21

PARTE II
REGOLAMENTO PER LA DISCIPLINA DEI SISTEMI DI VIDEOSORVEGLIANZA DEL COMUNE DI BAGNO DI ROMAGNA

Articolo 1 – Oggetto e liceità del trattamento dei dati personali pag. 22
Articolo 2 – Principi generali pag. 23
Articolo 3 – Soggetti pag. 25
Articolo 4 – Informazioni agli interessati pag. 26
Articolo 5 – Finalità dei trattamenti di dati personali e architettura degli impianti presenti pag. 27
Articolo 6 – Raccolta e trattamento dei dati personali pag. 30
Articolo 7 – Conservazione dei dati pag. 31
Articolo 8 – Diritti dell'interessato pag. 32
Articolo 9 – Accesso ai filmati pag. 33
Articolo 10 – Sicurezza dei dati pag. 34
Articolo 11 – Cessazione del trattamento dei dati pag. 35
Articolo 12 – Tutela amministrativa e giurisdizionale pag. 35
Articolo 13 – Sistemi di intelligenza artificiale pag. 35
Articolo 14 – Provvedimenti attuativi pag. 36
Articolo 15 – Norme finali e transitorie pag. 37

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 Bagno di Romagna, 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"), 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 Bagno di Romagna.

Articolo 2 – Finalità del trattamento

1. I dati personali sono trattati dal Comune di Bagno di Romagna, 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 Bagno di Romagna.

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 Bagno di Romagna, 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 e/o Responsabili di P.O., 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";
- **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 Bagno di Romagna, 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 e/o

Responsabili di P.O. 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 Bagno di Romagna 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 Bagno di Romagna 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 e/o Responsabili di P.O. 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 dei 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 III - 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 Bagno di Romagna 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.

5. 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 9 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 riguardanti la notifica di violazioni dei dati personali (data breach) adottate dalle autorità competenti in materia.

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 LA DISCIPLINA DEI SISTEMI DI VIDEOSORVEGLIANZA DEL COMUNE DI BAGNO DI ROMAGNA

Articolo 1 – Oggetto e liceità del trattamento dei dati personali

1. Il presente regolamento disciplina gli aspetti relativi ai trattamenti di dati personali eseguiti dal Comune di Bagno di Romagna (da ora solo "Comune") nel proprio territorio, mediante sistemi di ripresa e sorveglianza a distanza, fissi o mobili, collegati o meno ad un centro di controllo. In particolare:
    a) il sistema di videosorveglianza e lettura targhe, nell'ambito del territorio di competenza;
    b) i sistemi di sorveglianza e ripresa video-fotografica per l'accertamento da remoto di violazioni alle norme della circolazione stradale, previsti dalla vigente normativa;
    c) i sistemi di ripresa installati anche a tutela del patrimonio e della sicurezza dei luoghi lavoro nei luoghi ove viene svolta la prestazione lavorativa del personale dipendente;
    d) sistemi di ripresa audio-video, indossabili (*bodycam*) e/o veicolari (*dashcam*);
    e) altri sistemi di ripresa, anche mobili e ricollocabili ovunque posizionati dal titolare.
2. Il presente regolamento ha lo scopo di stabilire norme tecniche e organizzative di dettaglio e di concorrere a definire la base giuridica, le finalità e i mezzi dei trattamenti.
3. I trattamenti dei dati personali di cui al presente regolamento, quando rientrano nell'ambito di applicazione del GDPR, sono eseguiti a norma dell'articolo 6, paragrafo 1, lettere c) ed e), per adempiere un obbligo legale al quale è soggetto il Comune e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune e, a norma del paragrafo 3 dello stesso articolo 6, si fondano su basi giuridiche stabilite dal diritto dell'ordinamento nazionale. Le operazioni di trattamento effettuate dalla Polizia Locale, quale autorità competente, per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, comprese la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, sono invece disciplinate dal Decreto legislativo 18 maggio 2018, n. 51, nei limiti delle attribuzioni previste dalla legge.
4. Il presente regolamento, quale atto amministrativo generale di cui all'articolo 12 del Decreto legislativo 14 marzo 2013, n. 33, valorizza la base giuridica dei trattamenti a norma dell'articolo 2-*ter*, comma 1, del Decreto legislativo 30 giugno 2003, n. 196.
5. Con il presente regolamento si garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di ripresa installati, gestiti e impiegati dal Comune nel proprio

territorio, si svolga nel rispetto dei diritti e delle libertà, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e alla protezione dei dati personali.

6. Per le definizioni di cui al presente regolamento si rimanda al Regolamento (UE) 2016/679, d'ora in poi solo "GDPR", al Decreto legislativo 30 giugno 2003, n. 196 (recante il "Codice in materia di protezione dei dati personali", così come modificato dal D.Lgs. 101/2018), al Decreto legislativo 18 maggio 2018, n. 51, al Regolamento (UE) 2024/1689, come modificato dal Regolamento (UE) 2026/1744, d'ora in poi "AI Act", e alla Legge 23 settembre 2025, n. 132 e provvedimenti attuativi, ove applicabili.
7. Il presente regolamento stabilisce norme di dettaglio finalizzate ad attuare i principi stabiliti dalla vigente normativa, con riguardo ai trattamenti eseguiti dal Comune.
8. Il Comune di Bagno di Romagna promuove la sottoscrizione di Patti per l'attuazione della sicurezza urbana, protocolli di intesa, convenzioni o accordi comunque denominati, con soggetti pubblici e soggetti privati, per la condivisione di sistemi di videosorveglianza al fine di garantire i più elevati livelli di sicurezza del territorio. È in ogni caso garantita, nei casi e per le finalità previste dalla normativa vigente, la comunicazione di dati all'Autorità giudiziaria e alle Forze di polizia, anche a norma dell'articolo 2-ter, comma 2, del D.Lgs. 196/2003. Gli accordi di cui al presente comma devono definire finalità, ruoli, modalità di accesso e misure idonee a tutelare la protezione dei dati personali.

Articolo 2 – Principi generali

1. Ai sensi della vigente normativa, i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, come da ultimo definita dall'articolo 4, dal Decreto-legge 20 febbraio 2017, n. 14, convertito con Legge 18 aprile 2017, n. 48, come "*il bene pubblico che afferisce alla vivibilità e al decoro delle città da perseguire anche attraverso interventi di riqualificazione anche urbanistica, sociale e culturale, e recupero delle aree o dei siti degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio la promozione* della cultura *del rispetto della legalità e l'affermazione di più elevati livelli di coesione sociale e convivenza civile, cui concorrono prioritariamente, anche con interventi integrati, lo Stato, le Regioni e Province autonome di Trento e di Bolzano e gli enti locali, nel rispetto delle rispettive competenze e funzioni*".
2. I trattamenti di dati personali di cui al presente articolo sono ispirati ai principi contenuti nell'articolo 5, del GDPR e, in particolare secondo:
   a) "liceità, correttezza e trasparenza": i dati personali trattati con i sistemi di cui all'articolo 1 del presente regolamento sono trattati in modo lecito, corretto e trasparente nei confronti

degli interessati;

b) "limitazione della finalità": i dati personali sono raccolti per finalità determinate, esplicite e legittime, individuate nel presente regolamento e nei conseguenti provvedimenti attuativi. L'elencazione delle finalità nel presente regolamento non consente l'utilizzo indistinto dei dati raccolti mediante ciascun sistema. Ogni sistema o classe di dispositivi è preventivamente associato alle specifiche finalità perseguite e i dati non sono successivamente trattati in modo incompatibile con tali finalità, salvo che una specifica disposizione normativa ne consenta il trattamento per una finalità ulteriore;

c) "minimizzazione dei dati": i dati personali trattati sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità. Al riguardo, i sistemi di cui all'articolo 1 del presente regolamento sono progettati con criteri di necessità e proporzionalità;

d) "esattezza": i dati personali sono raccolti e trattati con modalità atte a garantirne l'esattezza e, ove necessario, l'aggiornamento. Qualora dati identificativi o informazioni rilevanti siano generati o associati mediante sistemi automatici, inclusi i sistemi di lettura targhe, sono adottate misure adeguate a verificarne l'affidabilità e la correttezza prima del loro utilizzo quando possano derivarne conseguenze per gli interessati;

e) "limitazione della conservazione": i dati personali sono conservati per il periodo di tempo strettamente necessario al conseguimento delle finalità. Qualora si rendessero necessari trattamenti ulteriori, per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o per fini statistici, devono essere adottate le misure previste dall'articolo 89, del GDPR;

f) "integrità e riservatezza": i sistemi di cui all'articolo 1 del presente regolamento e i relativi trattamenti di dati sono progettati al fine di garantire adeguata sicurezza dei dati personali, con l'implementazione di misure tecniche e organizzative adeguate alla protezione dei dati stessi da operazioni non autorizzate o illecite, dalla perdita, distruzione, danneggiamento, anche accidentali.

3. Il Comune, quale titolare del trattamento, in ottemperanza al principio di "responsabilizzazione" si impegna a comprovare il costante rispetto dei principi sopra specificati.
4. Il Comune progetta i trattamenti di dati personali eseguiti mediante i sistemi di cui all'articolo 1 del presente regolamento, adottando mezzi e misure tecniche e organizzative adeguate a garantire la conformità del trattamento ai principi, la protezione dei dati personali e la tutela dei diritti e libertà delle persone, sin dalla progettazione e per impostazione predefinita.
5. I trattamenti di cui al presente regolamento devono altresì essere eseguiti nel rispetto del D.Lgs. 51/2018, laddove applicabile.
6. Al fine di garantire la conformità dei trattamenti di cui al presente regolamento, il Comune

effettua, per ciascuno di essi, una Valutazione d'impatto sulla protezione dei dati personali di cui all'articolo 35 del GDPR e, laddove applicabile, di cui all'articolo 23 del D.Lgs. 51/2018, secondo le condizioni previste dalla normativa applicabile. La Valutazione è riesaminata quando intervengano modifiche delle finalità, delle modalità di trattamento, dell'architettura tecnica o delle funzionalità software suscettibili di incidere sui rischi per i diritti e le libertà delle persone. Il Responsabile della protezione dei dati è consultato nei casi e con le modalità previste dalla normativa vigente.

Articolo 3 – Soggetti

1. Titolare del trattamento dei dati personali di cui al presente regolamento è il Comune di Bagno di Romagna.
2. Per l'esecuzione di operazioni di trattamento per conto del titolare, il Comune può nominare uno o più responsabili del trattamento a norma dell'articolo 28 del GDPR, che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a garantire la conformità del trattamento. Qualora il responsabile debba essere individuato in un soggetto privato, l'affidamento avviene nel rispetto delle procedure previste dalla vigente normativa.
3. Designato al trattamento dei dati personali di cui al presente regolamento è il Responsabile del Settore Affari Generali nel cui ambito è inserito l'Ufficio di Polizia Locale. Gli altri Responsabili per tutti gli altri sistemi.
4. Per trattamenti di dati personali mediante sistemi di ripresa audio-video, installati in luoghi ove viene svolta la prestazione lavorativa del personale dipendente, il titolare può designare il Responsabile del Settore amministrativo competente.
5. I designati, nell'ambito delle funzioni e responsabilità di cui all'articolo 107 del Decreto legislativo 18 agosto 2000, n. 267, procedono a:
   a) individuare e nominare, con proprio provvedimento, gli autorizzati di cui al comma 6 alla gestione dei sistemi nel numero ritenuto sufficiente a garantire il corretto funzionamento e svolgimento del trattamento;
   b) fornire agli autorizzati di cui al comma 6, con l'atto di nomina le istruzioni necessarie allo svolgimento del ruolo specifico, anche per mezzo dei disciplinari operativi di cui all'articolo 14, comma 2;
   c) nominare, con atto scritto, i responsabili del trattamento di cui al comma 2, a norma dell'articolo 28 del GDPR e, in particolare, i soggetti individuati per lo svolgimento di compiti di assistenza/manutenzione e di amministrazione di sistema;
   d) svolgere gli adempimenti e predisporre i documenti previsti dalla vigente normativa, incluse le informazioni agli interessati, le Valutazioni d'impatto sulla protezione dei dati personali, i

disciplinari operativi e ogni altro atto necessario alla corretta esecuzione dei trattamenti, acquisendo il parere del Responsabile della protezione dei dati nei casi previsti;

e) adottare, con proprio provvedimento, i documenti e gli atti gestionali di cui alla precedente lettera d), nell'ambito delle funzioni e responsabilità attribuite.

6. Gli autorizzati, a norma dell'articolo 29 del GDPR, accedono e trattano i dati personali sotto l'autorità del titolare. Il designato, secondo criteri organizzativi, individua gli autorizzati in numero sufficiente a garantire la gestione dei sistemi con adeguata continuità, efficienza e efficacia. Gli autorizzati al trattamento sono dotati di credenziali personali di autenticazione al sistema.
7. Con l'atto di nomina di cui al comma 5, lettera a), ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo. In ogni caso, prima di svolgere operazioni di trattamento, essi sono istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa in materia e sulla disciplina di cui al presente regolamento e dei conseguenti provvedimenti attuativi.
8. Qualora il Comune, per l'esecuzione di uno o più dei trattamenti di cui al presente regolamento, determini congiuntamente le finalità e i mezzi con altri titolari, questi sono contitolari del trattamento e i relativi rapporti sono disciplinati con apposito accordo ai sensi della normativa applicabile. La mera condivisione dell'infrastruttura, la messa a disposizione dei dati o l'accesso ai sistemi da parte di altri soggetti pubblici, incluse le Forze di polizia, non determinano di per sé una contitolarità del trattamento.

Articolo 4 – Informazioni agli interessati

1. I soggetti interessati che stanno per accedere in una zona soggetta a riprese nell'ambito dei trattamenti di cui all'articolo 1, sono informati mediante informative di "primo livello", costituite da cartelli contenenti le informazioni previste dalla vigente normativa e dalle linee guida in materia. Sul cartello devono essere indicate le modalità per raggiungere l'informativa di "secondo livello", anche attraverso QR-code o altri sistemi analoghi.
2. In relazione alla presenza di più dispositivi di ripresa e alla vastità dell'area videoripresa, le informative di "primo livello" sono installate in modo da essere visibili agli interessati prima che possano accedere al raggio d'azione delle telecamere.
3. Sul sito istituzionale del Comune di Bagno di Romagna, è presente un'apposita sezione dedicata nella quale vengono pubblicate le informative di "secondo livello", nonché ogni altra informazione utile all'esercizio dei diritti degli interessati, previsti dalla vigente normativa.
4. In aggiunta alle modalità di pubblicazione di cui al precedente comma 3, le stesse informazioni possono essere messe a disposizione degli interessati anche con altri sistemi idonei. Quando

sistemi o dispositivi perseguono finalità differenti, le informazioni sono strutturate in modo da consentire all'interessato di comprendere il trattamento effettivamente svolto mediante lo specifico sistema. Per i sistemi che comportano il trattamento di dati personali dei lavoratori, il Comune rende agli stessi una specifica informativa, distinta da quella rivolta ai soggetti ripresi, ove necessario in relazione alle caratteristiche e alle finalità del trattamento.

Articolo 5 – Finalità dei trattamenti di dati personali e architettura degli impianti presenti

1. Le finalità perseguite mediante l'attivazione dei sistemi di cui al presente regolamento sono conformi alle funzioni istituzionali attribuite ai Comuni dalla normativa vigente. Ciascun sistema o classe di dispositivi è previamente associato, mediante i provvedimenti attuativi, il disciplinare operativo e la relativa Valutazione d'impatto, alle specifiche finalità per le quali è utilizzato. L'elencazione delle finalità contenuta nel presente articolo non costituisce autorizzazione generale all'utilizzo dei dati raccolti da un sistema per finalità diverse o ulteriori rispetto a quelle originariamente determinate.
2. L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte delle forze di polizia a competenza generale, dovrà essere specificamente disciplinato con appositi accordi di cui all'articolo 1, comma 8, del presente regolamento.
3. Il trattamento dei dati personali eseguito mediante i sistemi di cui all'articolo 1 del presente regolamento è effettuato dal Comune, attraverso le strutture e il personale autorizzato nell'ambito delle rispettive competenze. In particolare, l'Ufficio di Polizia Locale tratta i dati personali per il perseguimento delle seguenti finalità:
   a) attuazione di un sistema di sicurezza integrata ai sensi dell'articolo 2, del D.L. 14/2017;
   b) finalità amministrative di tutela della sicurezza urbana, a norma dell'articolo 6, comma 7, del Decreto-legge 23 febbraio 2009, n. 11, convertito dalla Legge 23 aprile 2009, n. 38, incluse le attività di prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria nei limiti in cui il relativo trattamento non ricada nelle finalità disciplinate dal D.Lgs. 51/2018; per queste ultime resta ferma la disciplina di cui alla successiva lettera g) e agli accordi previsti dal presente articolo;
   c) tutela della sicurezza stradale, intesa quale tutela dell'incolumità degli utenti della strada e alla gestione della viabilità, con particolare riferimento ai compiti di polizia stradale affidati alla Polizia Locale. Nello specifico:
      1) contrasto alla "pirateria stradale": assicurazione di prove per l'individuazione dei responsabili in caso di omissione di soccorso o fuga a seguito di incidente stradale;
      2) ricostruzione della dinamica degli incidenti stradali: utilizzo delle riprese per la

ricostruzione di incidenti stradali, con danni a cose o con danni a cose e persone, al fine di assicurare le fonti di prova e, quando il sistema sia stato legittimamente configurato anche per la pertinente finalità stradale o una specifica disposizione normativa consenta il trattamento, fornire supporto all'accertamento delle violazioni amministrative alle norme della circolazione stradale a seguito dell'istruttoria dell'incidente, a norma dell'articolo 13 della Legge 24 novembre 1981, n. 689. Resta comunque escluso ogni utilizzo per finalità di accertamento automatico delle violazioni in assenza di specifica previsione normativa e dei requisiti tecnici eventualmente richiesti dalla disciplina di settore;

3) accertamento delle violazioni previste dall'articolo 201 comma 5-*quater* del Decreto legislativo 30 aprile 1992, n. 285;
4) supporto all'accertamento della regolarità amministrativa dei veicoli e dei documenti di circolazione, esclusivamente in funzione della contestazione immediata da parte degli operatori su strada, con esclusione di ogni accertamento e sanzionamento da remoto;
5) supporto all'attività operativa delle pattuglie in servizio di polizia stradale;
6) monitoraggio dei flussi di traffico: analisi delle criticità della rete viaria per la prevenzione degli incidenti e la protezione dei soggetti vulnerabili.

d) tutela del patrimonio comunale (strutture, arredi urbani,…);
e) tutela ambientale e accertamento degli illeciti amministrativi di competenza comunale, compresi quelli in materia di polizia amministrativa e di conferimento e abbandono di rifiuti di cui all'articolo 255, commi 1.2 e 1-bis, del Decreto legislativo 3 aprile 2006, n. 152, accertabili a norma dell'articolo 13 della Legge 689/1981 e dell'articolo 255, comma 1-ter, del medesimo decreto;
f) attività di protezione civile e di tutela della sanità locale, intese come interventi finalizzati alla prevenzione e alla gestione delle emergenze;
g) prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nei limiti delle funzioni attribuite alla Polizia Locale quale autorità competente ai sensi del D.Lgs. 51/2018, incluso il ricorso all'arresto in flagranza o in flagranza differita nei casi previsti dalla legge.

4. Con accordi di cui all'articolo 1, comma 8, del presente regolamento, il Comune di Bagno di Romagna e il Prefetto definiscono altresì i termini secondo i quali i dati raccolti dai sistemi di cui all'articolo 1, comma 1, lettera a), del presente regolamento sono resi disponibili dal Comune alle Forze di polizia, che possono trattare i dati personali, per finalità di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, di cui all'articolo 1,

comma 2, del D.Lgs. 51/2018.

5. Per le finalità di cui al comma precedente, le amministrazioni da cui dipendono le Forze di polizia sono autonomi titolari dei trattamenti dei dati personali raccolti e messi a disposizione dal Comune. Tali trattamenti sono eseguiti dai competenti uffici e reparti territoriali individuati con l'accordo di cui al comma precedente o con altro atto specifico. La condivisione dell'infrastruttura tecnologica non comporta, di per sé, contitolarità dei trattamenti.
6. I trattamenti di dati personali eseguiti mediante sistemi di cui all'articolo 1, comma 1, lettera b) del presente regolamento, sono eseguiti esclusivamente per finalità di accertamento da remoto di violazioni alle norme della circolazione stradale, nei casi consentiti, tramite strumenti tecnologici omologati o approvati, secondo la vigente normativa in materia.
7. I trattamenti di dati personali eseguiti mediante sistemi di cui all'articolo 1, comma 1, lettere c) e d), quando effettuati nell'ambito di applicazione del GDPR, sono eseguiti esclusivamente per le seguenti finalità, nel rispetto, ove applicabile, dell'articolo 4 della Legge 20 maggio 1970, n. 300:
   a) tutela della sicurezza del lavoro;
   b) tutela del patrimonio dell'Amministrazione;
   c) esigenze organizzative connesse alla documentazione dell'attività istituzionale.
8. Resta distinto l'eventuale impiego dei sistemi di cui all'articolo 1, comma 1, lettera d), per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali: tale impiego costituisce autonomo trattamento disciplinato dal D.Lgs. 51/2018, nei limiti delle attribuzioni della Polizia Locale. Presupposti di attivazione, soggetti autorizzati, modalità di accesso, tempi di conservazione e misure di sicurezza sono definiti in una specifica Valutazione d'impatto e nel relativo disciplinare operativo.
9. Il Comune promuove, per quanto di propria competenza, la partecipazione di soggetti privati secondo quanto previsto dall'articolo 1, comma 8, del presente regolamento, anche tramite formule di partenariato pubblico-privato, finalizzate all'implementazione dei sistemi, per il solo perseguimento delle finalità specificate dal presente articolo. Gli interventi di cui al presente comma devono, in ogni caso, essere eseguiti nel rispetto della vigente normativa e con la puntuale definizione dei ruoli delle parti coinvolte. Il contributo economico, la cessione o la messa a disposizione di apparati da parte di soggetti privati non attribuiscono agli stessi alcun diritto di accesso, visione, estrazione o ingerenza sulle immagini e sui dati trattati dal Comune, salvo che ciò sia espressamente previsto dalla legge e formalmente disciplinato.
10. Nel rispetto della vigente normativa e per il perseguimento delle pertinenti finalità indicate nel presente articolo, l'Ufficio di Polizia Locale può dotarsi di sistemi di ripresa di cui all'articolo 1, comma 1, lettera e), quali droni, telecamere riposizionabili, anche del tipo "fototrappola", e altri

dispositivi mobili. L'installazione e l'impiego di tali sistemi devono in ogni caso avvenire conformemente alla vigente normativa e le relative modalità di impiego sono stabilite con specifico disciplinare operativo di cui all'articolo 14, comma 2.

Articolo 6 – Raccolta e trattamento dei dati personali

1. I trattamenti eseguiti con i sistemi di cui all'articolo 1, comma 1, lettere a), b) e e), del presente regolamento, riguardano i dati personali raccolti attraverso riprese video e immagini di telecamere di videosorveglianza e di lettura targhe installate in luoghi pubblici e aperti al pubblico sul territorio comunale. I dati personali trattati, sono costituiti dalle riprese relative a persone fisiche, targhe di veicoli, coordinate di luogo e di tempo, nonché ogni altra informazione che possa rendere identificabili le persone.
2. I sistemi di cui al comma precedente possono prevedere l'impiego di telecamere dotate di funzionalità di brandeggio, zoom, adeguamento delle riprese alle condizioni di luce ambientale, conteggio di veicoli o persone, analisi video e allertamento, attivabili sia manualmente dagli operatori autorizzati, sia attraverso algoritmi preimpostati, in ogni caso nel rispetto dei principi di cui all'articolo 2. Le circostanze e le modalità di attivazione delle funzionalità sono specificate nel disciplinare operativo di cui all'articolo 14, comma 2. L'introduzione o l'attivazione di nuove funzionalità software suscettibili di modificare natura, finalità, categorie di dati, modalità del trattamento o livello di rischio è preventivamente censita e valutata ai fini dell'eventuale aggiornamento dei provvedimenti attuativi e della Valutazione d'impatto.
3. I dati raccolti e trattati con i sistemi di cui all'articolo 1, comma 1, lettera c), del presente regolamento, sono costituiti dalle riprese video relative a persone fisiche, lavoratori dipendenti del Comune di Bagno di Romagna e utenti, che accedono alle sedi comunali o comunque ai luoghi in cui avviene la prestazione lavorativa dei dipendenti del Comune.
4. I dati raccolti e trattati con i sistemi di cui all'articolo 1, comma 1, lettera d), del presente regolamento, sono costituiti dalle riprese audio-video relative a persone fisiche, personale di Polizia Locale del Comune e utenti. Le riprese potranno essere avviate solo nei casi specificati nel disciplinare di cui all'articolo 14, comma 2, e limitate alle effettive esigenze.
5. Nei casi di cui ai commi precedenti, sono inoltre trattati i dati di log dei soggetti autorizzati ad accedere ai sistemi.
6. I sistemi di cui al presente regolamento, ove previsto dalla relativa configurazione tecnica e dalle finalità perseguite, possono essere collegati alla Centrale Operativa della Polizia Locale per la visione in diretta e/o delle registrazioni da parte dei soggetti autorizzati.
7. I sistemi di cui al presente regolamento possono, in relazione a circostanze concrete e

incidentali, comportare il trattamento di categorie particolari di dati personali di cui all'articolo 9 del GDPR. Nell'ambito di applicazione del GDPR, il trattamento di tali dati può avvenire esclusivamente nei casi e nei limiti previsti dal paragrafo 2 del medesimo articolo e dalla pertinente normativa nazionale.

8. Nell'ambito di applicazione del GDPR, l'eventuale trattamento di dati personali relativi a condanne penali e reati è eseguito nel rispetto dell'articolo 10 del GDPR e della pertinente normativa nazionale. Per i trattamenti effettuati per le finalità di cui all'articolo 1, comma 2, del D.Lgs. 51/2018, si applica invece la disciplina prevista dal medesimo decreto legislativo.
9. Per i trattamenti soggetti al D.Lgs. 51/2018 il Comune assicura altresì, in quanto applicabili, la distinzione tra le diverse categorie di interessati e la verifica della qualità dei dati (articolo 4), i limiti al trattamento di categorie particolari di dati, inclusi i dati biometrici (articolo 7), nonché le garanzie in materia di processi decisionali automatizzati (articolo 8 del medesimo decreto).

Articolo 7 – Conservazione dei dati

1. I dati personali oggetto dei trattamenti di cui al presente regolamento, fatta eccezione per quanto previsto dai commi seguenti e dai provvedimenti attuativi adottati in relazione a specifici trattamenti, sono conservati ordinariamente per un periodo di sette giorni dalla rilevazione.
2. I dati personali oggetto dei trattamenti di cui all'articolo 1, comma 1, lettera b), sono conservati per il periodo strettamente necessario alla specifica finalità di accertamento, individuato nel relativo disciplinare operativo e nella Valutazione d'impatto. L'eventuale previsione di un termine fino a novanta giorni deve essere specificamente motivata in relazione alle caratteristiche del trattamento, alla normativa di settore e alle concrete esigenze di contestazione, gestione della sanzione e dell'eventuale contenzioso.
3. I dati personali oggetto dei trattamenti di cui all'articolo 1, comma 1 lettera c) sono conservati ordinariamente per un periodo di settantadue ore.
4. Con i provvedimenti di cui all'articolo 14, comma 1, lettera b), del presente regolamento, nel rispetto dei principi di "minimizzazione" e "limitazione della conservazione", possono essere stabiliti termini diversi di conservazione, in relazione a specifiche esigenze connesse al trattamento e, comunque, non superiori al periodo di tempo strettamente necessario al conseguimento delle finalità. Per bodycam, dashcam e altri dispositivi mobili, i termini sono definiti nel relativo disciplinare operativo e nella Valutazione d'impatto, tenendo conto della finalità, delle modalità di attivazione e dell'eventuale verificarsi di eventi rilevanti.
5. Al termine del periodo di conservazione stabilito i sistemi provvedono alla cancellazione automatica mediante sovrascrittura, ove tecnicamente possibile, e, in ogni caso, con modalità

tali da rendere non più utilizzabili i dati cancellati.

6. È fatta salva la conservazione per ulteriori periodi di tempo quando ciò sia necessario in forza di una richiesta dell'Autorità giudiziaria o della polizia giudiziaria oppure, nei limiti consentiti dalla normativa applicabile, per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Le operazioni di preservazione, estrazione e successiva cancellazione sono tracciate secondo le modalità definite nel disciplinare operativo.

Articolo 8 – Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto di esercitare i diritti previsti dal GDPR e, in particolare:
   a) di ottenere dal titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, di accedere ai dati personali e di ottenere le informazioni indicate nell'articolo 15, del GDPR;
   b) di ottenere la rettifica dei dati personali inesatti ai sensi dell'articolo 16, del GDPR;
   c) alla cancellazione nei casi previsti dall'articolo 17, del GDPR;
   d) alla limitazione di trattamento nei casi previsti dall'articolo 18, del GDPR. Tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro;
   e) di opporsi, nei casi previsti dall'articolo 21, del GDPR, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.
2. L'interessato ha altresì diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, al di fuori dei casi previsti dall'articolo 22, paragrafo 2, del GDPR.
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 di protezione.
4. Laddove applicabile, l'interessato ha altresì la possibilità di esercitare i diritti previsti dal D.Lgs. 51/2018.
5. Le istanze sono presentate al titolare o al designato al trattamento.
6. Al solo fine di garantire l'esercizio concreto dei diritti il titolare mette a disposizione degli interessati specifiche indicazioni, anche tramite il sito web istituzionale.

Articolo 9 – Accesso ai filmati

1. Al di fuori dell'esercizio dei diritti di cui all'articolo precedente, le riprese possono essere oggetto dell'accesso ai documenti previsto dall'articolo 22 e seguenti della Legge 7 agosto 1990, n. 241.
2. Nei casi di cui al comma 1, l'istanza deve essere formulata per iscritto, con i contenuti e le modalità previste dalla vigente normativa e presentata al titolare o al designato al trattamento.
3. In considerazione dei tempi di conservazione dei dati personali di cui all'articolo 7 del presente regolamento, l'evasione dell'istanza può essere garantita solo nel caso in cui questa pervenga in modo tempestivo, tenuto comunque conto delle esigenze organizzative e delle circostanze concrete. Decorso il termine di conservazione, i filmati non sono più detenuti dall'Amministrazione. La presentazione di un'istanza di accesso non determina automaticamente la conservazione dei filmati oltre i termini ordinari; ove ricorrano idonei presupposti giuridici, il designato può disporne la tempestiva preservazione secondo quanto previsto dall'articolo 7 e dal relativo disciplinare operativo.
4. Per attività di indagine, l'Autorità giudiziaria e la polizia giudiziaria possono richiedere e acquisire copia dei filmati, delle immagini e delle altre informazioni raccolte con i sistemi di cui al presente regolamento, in formato digitale. Le modalità di rilascio sono stabilite con i provvedimenti di cui all'articolo 14, comma 2. Gli autorizzati al trattamento documentano le operazioni eseguite al fine di evadere la richiesta.
5. Nell'ambito delle investigazioni difensive e dell'attività investigativa preventiva di cui all'articolo 391-*novies*, del codice di procedura penale, il difensore, a norma dell'articolo 391-*quater*, dello stesso codice, può richiedere e acquisire copia delle riprese in formato digitale previo pagamento delle relative spese previste.
6. Le operazioni necessarie all'estrapolazione e consegna dei filmati dovranno essere tracciate a cura dell'autorizzato al trattamento dei dati, che provvederà ad annotare le operazioni eseguite al fine di garantire la genuinità dei dati stessi.
7. Per il perseguimento di fini istituzionali possono essere divulgate immagini provenienti dai sistemi di cui al presente regolamento, previa anonimizzazione di ogni dato che consenta l'identificazione delle persone e comunque nel rispetto della dignità, dei diritti e delle libertà degli interessati. La divulgazione è omessa qualora sussistano ulteriori ragioni che la rendano inopportuna. I presupposti per la divulgazione sono valutati caso per caso dal designato.
8. Fatta eccezione per le ipotesi di cui al comma 4, l'accesso ai filmati di cui al presente articolo, è soggetto al pagamento delle tariffe individuate con apposita deliberazione della Giunta comunale.
9. Con disciplinare operativo di cui all'articolo 14, comma 2, è attuato quanto previsto dal

presente articolo.

Articolo 10 – Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati su infrastrutture e sistemi informatici nella disponibilità del Comune, anche mediante servizi in cloud o servizi messi a disposizione da soggetti terzi formalmente individuati secondo la normativa applicabile. In ogni caso, il Comune mantiene il controllo giuridico e organizzativo dei dati personali e adotta misure di sicurezza fisica e informatica adeguate, finalizzate a garantirne riservatezza, integrità, disponibilità e resilienza. I rapporti con i fornitori disciplinano almeno ubicazione dei dati, eventuali subfornitori, accessi di assistenza, copie di backup, restituzione e cancellazione dei dati, nonché ogni eventuale trasferimento o accesso da Paesi terzi.
2. Nel caso di server presenti negli immobili comunali, questi devono essere ospitati in locali idonei secondo la vigente normativa.
3. L'accesso fisico o logico ai server e alle infrastrutture è consentito al solo personale autorizzato, nonché ai responsabili del trattamento di cui all'articolo 3, comma 2, per le sole operazioni di cui sono incaricati. Ogni accesso deve essere autorizzato e documentato secondo modalità idonee a garantirne la tracciabilità.
4. L'accesso alle riprese è consentito al solo personale autorizzato tramite postazioni client installate in locali in cui è consentito l'accesso al solo personale di cui al comma 3.
5. L'accesso ai locali di cui al presente articolo, può essere consentito temporaneamente, comunque per il tempo strettamente necessario, a personale incaricato di manutenzione e/o pulizia dei locali, nonché ad altri soggetti per motivi istituzionali. In tali ipotesi, l'accesso ai locali deve avvenire sotto la sorveglianza del designato e/o degli autorizzati e essere debitamente documentato. È in ogni caso escluso l'accesso ai sistemi e ogni altra operazione che possa pregiudicare, anche potenzialmente la protezione dei dati personali.
6. L'accesso fisico agli ambienti di cui al presente articolo è consentito agli autorizzati anche mediante sistemi di controllo elettronico degli accessi.
7. La gestione e l'utilizzo dei sistemi aventi finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali è riservata al solo personale di Polizia Locale e delle Forze di polizia, aventi qualifica di ufficiali o agenti di polizia giudiziaria ai sensi dell'articolo 57 del codice di procedura penale.
8. I sistemi devono essere forniti di log idonei a documentare gli accessi e le operazioni rilevanti. I log di accesso sono conservati ordinariamente per un periodo di sei mesi, salvo diverso termine motivato dalla Valutazione d'impatto o dalla normativa applicabile. Per i trattamenti di cui al D.Lgs. 51/2018 le registrazioni assicurano quanto previsto dall'articolo 21 del medesimo

decreto, comprese la tracciatura delle consultazioni e delle comunicazioni e l'identificazione del soggetto che vi ha proceduto.

9. Il designato può adottare ogni altra misura ritenuta necessaria al fine di evitare accessi abusivi ai locali, ai sistemi e ai dati personali. In relazione al rischio e alle caratteristiche della soluzione tecnica, sono adottate misure quali autenticazione forte, segregazione dei privilegi, cifratura e gestione controllata delle chiavi crittografiche. Le modalità di generazione, custodia e disponibilità delle chiavi e delle credenziali privilegiate devono garantire al Comune un effettivo governo del trattamento ed evitare che il fornitore disponga di un controllo esclusivo incompatibile con le responsabilità del titolare. Gli eventuali accessi del fornitore ai dati in chiaro devono essere limitati ai casi strettamente necessari, previamente autorizzati e tracciati.
10. Il Comune adotta una specifica procedura per la gestione degli incidenti e delle violazioni di dati personali (data breach), che garantisce l'attuazione degli obblighi previsti dal GDPR e, laddove applicabile, dal D.Lgs. 51/2018.

Articolo 11 – Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, dei trattamenti di dati personali di cui al presente regolamento, i dati personali sono distrutti, secondo quanto previsto dalla vigente normativa.
2. Alla cessazione del trattamento i dati sono cancellati in modo sicuro, salvi la conservazione o il versamento espressamente previsti dalla legge, anche in materia di archivi, ovvero la cessione all'Autorità competente nei casi normativamente stabiliti.

Articolo 12 – Tutela amministrativa e giurisdizionale

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli articoli 77 e seguenti del Regolamento (UE) 2016/679 e, laddove applicabili, dal Capo V del D.Lgs. 51/2018.
2. Il responsabile del procedimento, ai sensi e per gli effetti del Capo II della Legge 241/90, è individuato nel designato al trattamento dei dati personali.

Articolo 13 – Sistemi di intelligenza artificiale

1. I sistemi di cui al presente regolamento possono essere dotati di sistemi di intelligenza artificiale. In tale ipotesi il Comune riveste, ove ne ricorrano i presupposti, il ruolo di "deployer", come definito dall'articolo 3, paragrafo 1, n. 4), del Regolamento (UE) 2024/1689.
2. L'uso di tali sistemi deve, in ogni caso, garantire la tutela dei diritti fondamentali delle persone.

3. Laddove i sistemi di intelligenza artificiale di cui al comma 1 siano utilizzati per lo svolgimento di "attività di contrasto", come definita dall'articolo 3, paragrafo 1, n. 46), del Regolamento (UE) 2024/1689, nell'ambito delle competenze della Polizia Locale, o comunque rientrino tra i sistemi classificati ad alto rischio ai sensi dell'articolo 6 e dell'Allegato III del medesimo Regolamento, il Comune assicura il rispetto degli obblighi applicabili secondo il relativo calendario normativo. In particolare, le sezioni 1, 2 e 3 del Capo III si applicano, per effetto del Regolamento (UE) 2026/1744, dal 2 dicembre 2027 ai sistemi di cui all'articolo 6, paragrafo 2, e all'Allegato III e dal 2 agosto 2028 ai sistemi di cui all'articolo 6, paragrafo 1, e all'Allegato I, ferma restando l'applicazione delle altre disposizioni già efficaci.
4. È in ogni caso proibito l'impiego di sistemi di intelligenza artificiale vietati, a norma dell'articolo 5, del Regolamento UE 2024/1689. L'impiego di tali sistemi è altresì escluso anche al ricorrere delle eccezioni previste dallo stesso articolo 5, paragrafo 1, lettera h), del medesimo Regolamento, qualora la normativa vigente non lo preveda espressamente.
5. Le funzionalità di analisi video, ricerca semantica negli archivi, riconoscimento o classificazione di soggetti, caratteristiche, fatti, comportamenti od oggetti, analisi predittiva, lettura automatizzata di targhe o di altre informazioni non determinano, per il solo fatto di essere realizzate mediante intelligenza artificiale, la classificazione automatica del sistema come ad alto rischio. Ogni sistema di intelligenza artificiale è preventivamente censito e classificato in relazione alla finalità prevista, alle concrete modalità di impiego e ai criteri stabiliti dall'articolo 6 e dall'Allegato III del Regolamento (UE) 2024/1689, incluse, ove applicabili, le condizioni di cui all'articolo 6, paragrafo 3.
6. In attuazione dell'articolo 4 del Regolamento (UE) 2024/1689, il Comune assicura un livello sufficiente di alfabetizzazione in materia di intelligenza artificiale al personale destinato all'impiego dei sistemi, tenendo conto delle conoscenze tecniche, dell'esperienza, dell'istruzione, della formazione e del contesto di utilizzo.
7. Il Comune adotta le misure tecniche e organizzative necessarie a garantire il corretto uso dei sistemi di intelligenza artificiale, la supervisione umana ove richiesta, la tracciabilità delle operazioni e la tutela dei diritti fondamentali delle persone, procedendo all'aggiornamento della documentazione di governance, delle Valutazioni d'impatto e degli altri adempimenti applicabili quando l'introduzione o la modifica di funzionalità di intelligenza artificiale incida sui trattamenti effettuati.

Articolo 14 – Provvedimenti attuativi

1. La Giunta comunale, nel rispetto di quanto disposto dal presente regolamento, con propria

deliberazione:

a) fornisce indirizzi relativi alla realizzazione e implementazione dei sistemi di cui al presente regolamento;
b) adotta atti amministrativi generali finalizzati a dare esecuzione al presente regolamento;
c) prende atto, ove connesse a interventi o progetti sottoposti alla propria approvazione, delle Valutazioni d'impatto sulla protezione dei dati personali di cui all'articolo 2, comma 6, ferma restando la competenza dei designati alla loro predisposizione e adozione nell'ambito delle rispettive funzioni;
d) approva gli accordi di cui all'articolo 1, comma 8, nonché ogni altro protocollo d'intesa, convenzione o accordo comunque denominato, finalizzato a garantire la condivisione dei sistemi di cui al presente regolamento.

2. Il Responsabile del Settore Affari Generali nel cui ambito è inserito l'Ufficio di Polizia Locale e gli altri designati di cui all'articolo 3, commi 3 e 4, adottano specifici disciplinari operativi per l'impiego dei sistemi di cui al presente regolamento, nell'ambito delle rispettive competenze.
3. I soggetti di cui al comma precedente provvedono altresì ad adottare tutti i provvedimenti gestionali finalizzati alla conformità dei trattamenti di cui al presente regolamento, inclusi gli atti indicati all'articolo 3, comma 5, le informative di cui all'articolo 4, le Valutazioni d'impatto e ogni altro adempimento ad essi attribuito dal presente regolamento o dalla normativa vigente, acquisendo il parere del Responsabile della protezione dei dati nei casi previsti.

Articolo 15 – Norme finali e transitorie

1. Dalla data di entrata in vigore del presente regolamento viene abrogato la Parte II ("Regolamento per l'installazione e l'utilizzo di impianti di videosorveglianza") del "Codice per il trattamento dei dati personali e la video sorveglianza" approvato con deliberazione del Consiglio comunale n. 8 del 15/04/2024. Resta in vigora la Parte I del medesimo Codice.
2. Fermi restando gli obblighi previsti dalla vigente normativa, entro sei mesi dall'entrata in vigore del presente regolamento i soggetti di cui ai commi 1 e 2 dell'articolo precedente sono tenuti a darvi attuazione.