



*Comune di Romanengo*  
*Provincia di Cremona*

\*\*\*\*\*

**REGOLAMENTO PER LA GESTIONE DELLA  
RISERVATEZZA DEI DATI PERSONALI**

**Approvato con D.C.C. n. 2 del 26.03.2021**

P.zza Matteotti n. 3 - 26014 ROMANENGO (CR)  
Cod. Fis. e Part. IVA 00325790194 - Telefono 0373 - 72117 - 72380 - Fax 72358  
PEC: [comune.romanengo@pec.regione.lombardia.it](mailto:comune.romanengo@pec.regione.lombardia.it)  
Mail: [protocollo@comune.romanengo.cr.it](mailto:protocollo@comune.romanengo.cr.it)  
Mail: [segreteria@comune.romanengo.cr.it](mailto:segreteria@comune.romanengo.cr.it)

**COMUNE DI ..ROMANENGO.....**

**Provincia di ..CREMONA.....**



**REGOLAMENTO  
PER LA GESTIONE  
DELLA RISERVATEZZA  
DEI DATI PERSONALI**



# INDICE

GLOSSARIO .....	1
<b>TITOLO I - PRINCIPI</b> .....	<b>4</b>
Art. 1 - Finalità .....	4
Art. 2 - Principi del trattamento .....	4
Art. 3 - Definizioni .....	5
<b>TITOLO II - SOGGETTI DEL TRATTAMENTO DEI DATI</b> .....	<b>6</b>
Art. 4 - Titolare del trattamento .....	6
Art. 5 - Responsabili del trattamento .....	6
Art. 6 - Competenze del Responsabile della protezione dei dati (DPO) .....	7
Art. 7 - Responsabili esterni di trattamento .....	8
<b>TITOLO III - TRATTAMENTO DEI DATI PERSONALI</b> .....	<b>10</b>
Art. 8 - Trattamento dati particolari 4 .....	10
Art. 9 - Principi del trattamento dei dati particolari e giudiziari .....	10
Art. 10 - Individuazione di interesse pubblico rilevante .....	11
Art. 11 - Pubblicazione web per obblighi di trasparenza .....	12
Art. 12 - Pertinenza delle informazioni contenenti dati personali .....	13
Art. 13 - Trattamento dei dati personali effettuato con sistemi di videosorveglianza .....	13
Art. 14 - Registro del trattamento .....	14
<b>TITOLO IV - DIRITTI DELL'INTERESSATO</b> .....	<b>14</b>
Art. 15 - Diritto di accesso ed alla portabilità dei dati .....	14
Art. 16 - Diritto di limitazione .....	15
Art. 17 - Diritto all'oblio .....	15
Art. 18 - Diritto alla rettifica dei dati .....	16
Art. 19 - Diritto di opposizione .....	16
Art. 20 - Obbligo di informativa <sub>s</sub> .....	16
Art. 21 - Contenuto dell'informativa .....	17
Art. 22 - Informativa per utilizzo di sistemi di videosorveglianza .....	18
Art. 23 - Consenso .....	18
<b>TITOLO VI - MISURE DI SICUREZZA (6)</b> .....	<b>18</b>
Art. 24 - Misure di sicurezza preventive .....	18
Art. 25 - D.P.I.A. .....	19
Art. 26 - Procedimento .....	20
Art. 27 - Consultazione preventiva del Garante della privacy .....	20
Art. 28 - Misure di sicurezza minime per trattamenti con strumenti elettronici ed informatici .....	21
Art. 29 - Misure per trattamenti non automatizzati .....	22

## TITOLO I - PRINCIPI

### **Art. 1 - Finalità**

1. Il presente regolamento disciplina le misure organizzative ed i processi interni di attuazione del Regolamento UE n. 679/2016 (GDPR.) ai fini del trattamento di dati personali per finalità istituzionali nel Comune di ..... di seguito Comune.
2. Ai fini del presente regolamento, per funzioni istituzionali si intendono quelle:
  - a) previste dalla legge, dallo statuto comunale e dai regolamenti;
  - b) esercitate in attuazione di convenzioni, accordi nonché sulla base degli strumenti di programmazione e pianificazione previsti dalla legislazione vigente;
  - c) svolte per l'esercizio dell'autonomia organizzativa, amministrativa e finanziaria dell'ente locale;
  - d) in esecuzione di un contratto con i soggetti interessati;
  - e) per finalità specifiche e diverse dai punti precedenti purché l'interessato esprima il consenso al trattamento.
3. Il presente regolamento è conforme alle norme e principi costituzionali nonché alle altre disposizioni vigenti in materia di privacy.

### **Art. 2 - Principi del trattamento**

1. Per le finalità indicate all'art. 1, il Comune effettua il trattamento dei dati personali nel rispetto dei diritti e libertà fondamentali delle persone fisiche nonché del diritto alla riservatezza ed all'identità di persone fisiche e giuridiche.
2. In attuazione del comma 1, i dati personali sono:
  - trattati in conformità delle norme di legge, cioè in modo lecito e con trasparenza nei confronti dell'interessato;
  - corretti, esatti ed aggiornati a seguito di intervenute variazioni;
  - solo quelli necessari e pertinenti allo scopo specifico, con la riduzione al minimo delle informazioni identificative; il trattamento va evitato laddove lo scopo specifico può essere raggiunto tramite dati anonimi;
  - trattati con adeguate misure di sicurezza in modo da evitare abusi o illeciti o perdita, distruzione o danno accidentale, in conformità del principio di integrità e riservatezza.
3. Relativamente al trattamento di dati personali di persone decedute, il diritto alla riservatezza si estingue con la morte del titolare. I diritti di cui al Titolo V del presente regolamento, in tali casi, possono essere esercitati da chi agisce per la tutela del defunto o per motivi familiari meritevoli di tutela.<sup>1</sup>

<sup>1</sup> Il Reg. UE n. 679/2016 non si applica alle persone decedute ma lascia liberi gli Stati membri di provvedere ed in merito il riferimento per la nostra legislazione è l'art. 9, co. 3, D.Lgs. n. 196/2003, da considerarsi ancora vigente. Per la giurisprudenza del Consiglio di Stato sopravvive una forma di tutela dei dati sensibili – come altre forme di tutela – anche dopo la morte, ma nelle forme specifiche e diverse previste dall'art. 9, co. 3, citato per la tutela del defunto e ragioni familiari meritevoli di protezione. (cfr. Consiglio di Stato, Sez. III, sentenza 12 giugno 2012, n. 3459)

## TITOLO II - SOGGETTI DEL TRATTAMENTO DEI DATI

### **Art. 4 - Titolare del trattamento**

1. Il Titolare del trattamento dei dati personali è il Comune rappresentato ai fini legali previsti dal Regolamento UE n. 679/2016 dal Sindaco pro-tempore<sup>1</sup>. Esso è il Responsabile per tutte le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati e può agire tramite un suo delegato<sup>2</sup> per le competenze attribuite dal presente regolamento.
2. Il Comune adotta tutte le misure tecniche ed organizzative idonee a garantire che il trattamento è conforme ai principi di cui all'art. 2 e ciò deve essere dimostrabile.
3. Tramite verifiche periodiche deve vigilare sulla osservanza delle istruzioni scritte impartite ai Responsabili e sul pieno rispetto delle vigenti disposizioni in materia di trattamento dati.
4. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, ogni Comune mantiene la titolarità dei propri dati e crea un accordo di nomina a Responsabile esterno ad ogni ente associato.

### **Art. 5 - Responsabili del trattamento**

Il Titolare del trattamento dei dati nomina<sup>2</sup>, con provvedimento motivato con Decreto Sindacale, il DPO (Data Protection Officer), un supervisore indipendente che deve essere obbligatoriamente designato da soggetti apicali (Sindaci) di tutte le pubbliche amministrazioni.

Le funzioni del DPO (contenute nell'articolo 39 del Regolamento UE 2016/679) riguardano principalmente la consulenza al titolare e ad eventuali responsabili del trattamento sul rispetto degli obblighi derivanti dal GDPR e dalla normativa nazionale, oltre a verificarne l'osservanza. Al DPO si chiede inoltre di cooperare con l'autorità di controllo e di esserne il punto di riferimento per facilitare l'accesso a documenti e informazioni riguardanti l'azienda o l'ente ed in ultimo, di collaborare con titolare e responsabili di settore, se richiesto, alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento.

I Responsabili di Settore sono anch'essi nominati tramite un provvedimento Sindacale e provvederanno, a loro volta, ad impartire istruzioni agli incaricati<sup>4</sup> sottoposti a seguito di un confronto con il DPO in carica.

2. Il nominativo nonché indirizzo Pec del DPO va pubblicato nel sito del Comune alla sezione Amministrazione trasparente.

3. Il DPO (Data Protection Officer – Responsabile della Protezione dei dati) è incaricato almeno dei seguenti compiti:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

<sup>2</sup> Il Garante privacy ha chiarito già nel parere 11 dicembre 1997 che il Titolare del trattamento per un ente locale è il Comune nel suo complesso rappresentato dal Sindaco. Il Comune, tuttavia, agisce di volta in volta con i suoi Responsabili. Il Segretario comunale non è il Titolare del trattamento ma può essere nominato Responsabile unico del trattamento.

2. Il Responsabile esprime parere non vincolante; l'eventuale adozione di condotta difforme da quella da lui suggerita va motivata.
3. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il DPO non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

### ***Art. 7 - Responsabili esterni di trattamento***

1. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del Responsabile del trattamento e le modalità di trattamento.
2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
  - tratti i dati personali secondo il regolamento in materia di privacy in vigore, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
  - garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
  - adotti tutte le misure richieste ai sensi dell'articolo 32;
  - rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
  - tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
  - assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

## TITOLO III - TRATTAMENTO DEI DATI PERSONALI

### *Art. 8 - Trattamento dati particolari <sup>4</sup>*

1. Gli uffici del Comune trattano i dati particolari, sensibili ai sensi dell'art. 9 del GDPR, che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, biometrici, relativi alla salute, alla vita sessuale ed i dati giudiziari:
  - per motivi di interesse pubblico rilevante come specificati nel successivo art. 12;
  - per un interesse vitale dell'interessato o di altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
  - se l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche;
  - per diritti dell'interessato in materia di diritto del lavoro e sicurezza sociale e protezione sociale autorizzato da norma di legge o contratto collettivo;
  - il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
  - Il trattamento è necessario ai fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici ed è proporzionato alla finalità perseguita;
2. In tutti i casi indicati vanno sempre previste misure di garanzia appropriate e specifiche per tutelare i diritti fondamentali e gli interessati. A tal fine si applicano le misure di sicurezza previste nei successivi artt. 26 e ss.
3. I dati particolari riguardanti lo stato di salute non devono essere divulgati.

### *Art. 9 - Principi del trattamento dei dati particolari e giudiziari*

1. I dati particolari di cui all'articolo precedente sono trattati sempre nel rispetto dei principi indicati nell'art 2, ovvero devono essere esatti, pertinenti, non eccedenti ed indispensabili rispetto alle finalità perseguite e sono aggiornati periodicamente.
2. I raffronti e le interconnessioni con altre informazioni sensibili e giudiziarie detenute dal Comune sono consentite soltanto previa verifica della loro stretta indispensabilità nei singoli casi ed indicazione scritta dei motivi che ne giustificano l'effettuazione. Lo stesso vale se le predette operazioni sono effettuate utilizzando anche dati di diversi titolari del trattamento, nonché la diffusione di dati sensibili e giudiziari, sono ammesse esclusivamente previa verifica nel rispetto dei limiti e con le modalità stabiliti dalle disposizioni legislative che le prevedono.
3. Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali (e consigliato per non tenere separato il regolamento per i dati sensibili e giudiziari). Al presente regolamento sono direttamente indicati le schede per il trattamento dei dati particolari, sensibili e giudiziari come individuate dal Garante.
4. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o dello Stato che preveda garanzie appropriate per i diritti e le libertà degli interessati.

<sup>4</sup> Gli artt. 10-12 del presente regolamento assorbono il regolamento dei dati sensibili e giudiziari (non più come regolamento separato quindi) e sono stati redatti tenendo a mente il provvedimento generale del Garante privacy del 30 giugno 2005 e lo schema tipo predisposto dall'Anci. L'art. 9 GDPR ridenomina la categoria dei dati sensibili come particolare e ne specifica meglio i casi in cui possono essere trattati.

## VOLONTARIATO E SERVIZI SOCIALI

Sono considerate di rilevante interesse pubblico le attività finalizzate all'applicazione della disciplina in materia di rapporti con le organizzazioni di volontariato, nella specie per quanto concerne l'erogazione di contributi, nonché:

- interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;
- interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;
- assistenza nei confronti di minori, anche in relazione a vicende giudiziarie.

## ATTIVITÀ DI PREDISPOSIZIONE DI ELEMENTI DI TUTELA IN SEDE AMMINISTRATIVA O GIURISDIZIONALE

Sono di rilevante interesse pubblico i trattamenti di dati effettuati in conformità di leggi o di regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi.

## RAPPORTI CON ENTI DI CULTO

Sono considerati di rilevante interesse pubblico i trattamenti strettamente necessari allo svolgimento dei rapporti istituzionali con gli enti di culto, con le confessioni e le comunità religiose.

### ***Art. 11 - Pubblicazione web per obblighi di trasparenza***

1. Il Comune effettua il trattamento di dati personali, contenuti in atti e documenti amministrativi, che devono essere pubblicati sul web per obblighi di trasparenza previsti dal D.Lgs. n.33/2013.
2. I documenti di cui al comma 1 sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione e vanno mantenuti aggiornati.
3. Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.
4. I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati particolari relativi alla vita sessuale non possono essere diffusi per finalità di trasparenza.
5. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.
6. I dati vanno pubblicati in formato di tipo aperto ai sensi dell'art. 68, D.Lgs. n. 82/2005 e sono liberamente riutilizzabili secondo la normativa vigente. I dati personali diversi dai dati sensibili e dai dati giudiziari, possono essere diffusi attraverso siti istituzionali, nonché trattati secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web.
7. I dati, le informazioni e i documenti di cui al comma 1, sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello dell'obbligo di pubblicazione.
8. Deroghe alla predetta durata temporale quinquennale sono previste:
  - a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;

### **Art. 14 - Registro del trattamento**

1. Il Titolare del trattamento istituisce e tiene aggiornato, in forma scritta ed in formato elettronico, coadiuvato dal DPO e dai Responsabili di settore designati un registro delle attività di trattamento svolte sotto la propria responsabilità.
2. Il Registro privacy del Titolare del trattamento deve contenere almeno le seguenti informazioni:
  - estremi identificativi e di contatto del Comune;
  - estremi identificativi e di contatto Responsabile della protezione dei dati;
  - finalità del trattamento;
  - descrizione delle categorie di interessati;
  - descrizione delle categorie di dati personali;
  - categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
  - eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale con documentazione delle garanzie in materia di privacy;
  - termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  - descrizione generale delle misure di sicurezza tecniche e organizzative adottate.
3. In caso di richiesta del Garante, il Registro privacy è messo immediatamente a disposizione.

## **TITOLO IV - DIRITTI DELL'INTERESSATO**

### **Art. 15 - Diritto di accesso ed alla portabilità dei dati**

1. L'interessato ha sempre diritto di ottenere dal Titolare del trattamento la conferma che sia in corso un trattamento dei dati personali che lo riguardano, di averne accesso e di acquisire le seguenti informazioni:
  - finalità del trattamento;
  - categoria di dati trattati;
  - i destinatari a cui i dati personali sono comunicati;
  - il periodo di conservazione dei dati previsto o se non è possibile, i criteri utilizzati per determinare tale periodo;
  - l'esistenza del proprio diritto a richiedere la rettifica o cancellazione del dato o la limitazione dei dati o di opporsi al loro trattamento;
  - l'esistenza di un processo automatizzato e della profilazione dei dati nonché informazioni sulla logica utilizzata.
2. La richiesta va inoltrata in forma scritta dall'interessato senza particolari formalità; in caso sia inoltrata con mezzi elettronici, salvo contraria indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.
3. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
4. I Responsabili del trattamento di settore, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, e se necessarie, anche al fine di identificarlo e,

5. In caso in cui i dati non siano diffusi pubblicamente e su siti web il Titolare del trattamento è tenuto ad avvisare i destinatari della cancellazione dei dati, salvo ciò non sia impossibile o richieda uno sforzo sproporzionato.

### ***Art. 18 - Diritto alla rettifica dei dati***

1. L'interessato ha diritto a chiedere previa richiesta scritta, la rettifica da parte del Comune, senza ingiustificato ritardo, dei dati personali inesatti che lo riguardano. La rettifica include anche la possibile integrazione dei dati avuto riguardo alla finalità del trattamento.
2. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
3. I Responsabili di settore, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, e se necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.

### ***Art. 19 - Diritto di opposizione***

1. L'interessato può presentare per iscritto richiesta di opposizione al trattamento dei dati personali che lo riguardano per motivi connessi alla sua situazione particolare, inclusa la profilazione.
2. Il Titolare del trattamento entro trenta giorni fornisce risposta all'interessato a seguito della valutazione della situazione: è consentito l'esercizio del diritto se non esistano comprovati motivi basati su norma di legge per procedere al trattamento prevalenti sugli interessi del richiedente o se si tratta di esercizio o accertamento di un diritto in sede giudiziaria.
3. Il termine di cui al precedente comma può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
4. I Responsabili di settore, sono tenuti a collaborare nel procedimento interno di verifica dei presupposti del diritto di opposizione.
5. In ogni comunicazione all'interessato deve essere inserito l'avviso in modo chiaro e separato dal restante contenuto dell'atto che questi può esercitare il diritto all'opposizione.

### ***Art. 20 - Obbligo di informativa***

1. Prima che inizi qualunque trattamento di dati personali il Titolare del trattamento fornisce all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti.
2. L'informativa privacy deve essere fornita per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.
3. Essa va effettuata:
  - in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, nel momento della raccolta dei dati;
  - in caso di dati personali non ottenuti presso l'interessato: 1) entro un termine ragionevole, massimo di un mese dalla raccolta (non registrazione) dei dati; 2) nel caso in cui i dati vadano

## **Art. 22 - Informativa per utilizzo di sistemi di videosorveglianza**

1. Nel caso di utilizzo di sistemi di videosorveglianza per finalità di sicurezza urbana, gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).
2. A tal fine può essere utilizzato un modello di informativa semplificata che poi rinvii a un testo contenente tutti gli elementi completi di cui all'articolo precedente, disponibile agevolmente senza oneri per gli interessati, sia sul sito internet dell'amministrazione comunale che nella sede della polizia municipale.
3. In ogni caso il Titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'articolo precedente.
4. Il supporto con l'informativa:
  - deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
  - deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
  - può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

## **Art. 23 - Consenso**

1. Il consenso al trattamento dei dati non è richiesto al Comune in quanto pubblica amministrazione se agisce per finalità istituzionali.
2. Il consenso può essere richiesto se il Comune agisce per specifiche finalità diverse da quelle istituzionali ai sensi dell'art. 1, comma 1, lett. e) del GDPR. In tal caso il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.
3. La richiesta di consenso deve essere comprensibile, facilmente accessibile, chiara e semplice.
4. Il consenso può essere revocato ed in tal caso la revoca non pregiudica la liceità del trattamento già effettuato.

## **TITOLO VI - MISURE DI SICUREZZA <sup>(6)</sup>**

### **Art. 24 - Misure di sicurezza preventive**

1. Il Comune deve adottare misure che soddisfino la protezione dei dati fin dalla progettazione e della protezione dei dati di default; ovvero, mette in atto misure tecniche ed organizzative adeguate sia prima del trattamento, sia nell'atto del trattamento stesso, indicate nel presente titolo.
2. Il Comune in particolare:
  - utilizza le tecniche di pseudonimizzazione dei dati personali;
  - tratta i soli dati necessari per ogni specifica finalità al fine di garantire la massima protezione dei dati attraverso il loro minimo trattamento;
  - custodisce e controlla i dati personali in modo da ridurre al minimo, mediante l'adozione di misure di sicurezza preventive, i rischi di distruzione, perdita, anche accidentale, di dati stessi, di accesso

- dati relativi a interessati vulnerabili considerato lo squilibrio di potere tra gli interessati ed il Comune;
- uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

6. Il Titolare se lo ritiene opportuno può procedere anche alla D.P.I.A. in caso ricorra anche uno solo dei requisiti sopra indicati e può individuare anche altri criteri di riscontro del rischio elevato in base alla specifica circostanza.

#### **Art. 26 - Procedimento**

1. Qualora ricorra un rischio elevato il Titolare del trattamento, chiede il parere del Responsabile della Protezione dei dati (DPO) e, se lo ritiene opportuno, degli stessi interessati.
2. La D.P.I.A. deve presentare il seguente contenuto minimo:
  - una descrizione dei trattamenti previsti e delle finalità del trattamento;
  - una valutazione della necessità e proporzionalità dei trattamenti;
  - una valutazione dei rischi per i diritti e le libertà degli interessati;
  - le misure previste per affrontare i rischi.
3. La D.P.I.A. può essere effettuata anche da un Responsabile del trattamento ma la responsabilità finale è del Titolare del trattamento.
4. In caso la D.P.I.A. non riesca a trattare in maniera sufficiente i rischi individuati, per quelli residui va effettuata, per tramite del Responsabile della protezione dei dati, la consultazione del Garante.

#### **Art. 27 - Consultazione preventiva del Garante della privacy**

1. Nei casi in cui si è proceduto nella valutazione di impatto sulla protezione dei dati ed è emerso che il Comune non riesce a trattare in maniera sufficiente tutti i rischi elevati, poiché ne restano ancora alcuni per questi ultimi residui, va consultato preventivamente il Garante per la privacy.
2. Il Comune tramite il Responsabile della protezione dei dati (DPO) ai sensi degli artt. 36 e 39, par. 1, lett. e), Regolamento UE n. 679/2016, invia richiesta di consultazione al Garante comunicando:
  - i dati dell'ente locale in quanto Titolare del trattamento ed i propri dati in quanto punto di contatto e referente per la consultazione;
  - le finalità ed i mezzi di trattamento previsti;
  - le misure di garanzia previste per proteggere i diritti e le libertà fondamentali degli interessati;
  - la valutazione di impatto sulla protezione dei dati in versione completa;
  - ogni altra informazione ritenuta necessaria.
3. Il Garante formula parere scritto entro otto settimane dal ricevimento della richiesta di consultazione nel caso in cui ritenga che il trattamento comunicato violi le norme sulla protezione dei dati ed in particolare qualora ritenga che il Comune non abbia sufficientemente attenuato o identificato il rischio. In base alla complessità del trattamento previsto il Garante può prorogare la sua risposta di un termine aggiuntivo di sei settimane informando il Responsabile della protezione dei dati, entro un mese dal ricevimento della richiesta di consultazione.

### ***Art. 29 - Misure per trattamenti non automatizzati***

1. Il Comune fornisce istruzioni scritte agli incaricati anche per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici, in particolare, per il controllo e la custodia, per intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
2. I documenti che contengano dati sensibili e giudiziari, sono controllati fino alla restituzione in modo che non accedano ad essi persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
3. L'accesso agli archivi contenenti dati particolari è controllato.
4. Le persone ammesse, dopo l'orario di chiusura, sono identificate e registrate e se mancano strumenti elettronici di controllo degli accessi agli archivi, questi vanno preventivamente autorizzati.

### ***Art. 30 - Misure per dati raccolti con sistemi di videosorveglianza***

1. I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
2. Occorre rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando – quando non indispensabili – immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
3. Devono quindi essere adottate almeno le seguenti specifiche misure tecniche ed organizzative:
  - in presenza di differenti competenze attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i già menzionati soggetti, designati incaricati o, eventualmente, Responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
  - laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
  - nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle già menzionate operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
  - qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo.

### **Art. 33 - Monitoraggio**

1. Il Comune verifica che vengano applicate le procedure interne e delle misure di sicurezza adottate in sede di audit e, precisamente che:

- venga fatto un uso corretto di mezzi informatici ai fini del trattamento dei dati personali, in particolare monitorando l'utilizzo delle password e gli accessi agli archivi elettronici contenenti dati personali con particolare attenzione ai dati sensibili;
- venga fatto un corretto utilizzo degli archivi cartacei che conservano i dati personali con particolare riguardo alla conservazione dei dati sensibili;
- vengano adeguatamente formati i dipendenti in modo diversificato in base alla modalità di trattamento cui sono preposti;
- ogni ufficio comunale tratti i dati secondo il principio di minimizzazione, ovvero, solo a ciò che sia strettamente necessario, si accerti dell'esattezza e correttezza dei dati e che conservi i dati nel rispetto dei termini indicati dalle norme, laddove presenti, o, in subordine per il tempo strettamente necessario al raggiungimento della finalità di trattamento;
- in caso di incidenti o violazioni come descritte al titolo successivo, siano applicate le misure correttive per porre riparo agli effetti negativi;
- che siano garantiti i diritti degli interessati e correttamente curate le istanze di accesso, cancellazione, limitazione del trattamento, rettifica nonché siano verificate le istanze di opposizione nonché i reclami eventualmente presentati al Garante;
- che vengano tenuti sempre aggiornati i contenuti delle informative e siano adattate alle esigenze dei differenti uffici e differenti trattamenti;
- che i documenti contenenti dati personali, presenti nel sito internet del Comune con particolare riferimento alla pubblicazione all'albo pretorio ed alla sezione Amministrazione Trasparente siano conformi ai tempi di pubblicazione previsti dall'art. 124, D.lgs. n. 267/2000 e D.lgs. n. 33/2013;
- che nelle ipotesi di utilizzo di sistemi di videosorveglianza vengano rispettate le specifiche misure di sicurezza come indicate negli artt. 12, 21, 29 del presente regolamento.

2. In caso di riscontro di non corretta applicazione del sistema di audit predisposto e delle norme sul trattamento dei dati personali, il Responsabile di trattamento insieme al Responsabile della Protezione dei dati predispone l'adozione di misure nuove correttive.

3. Se in sede di monitoraggio

insieme alla collaborazione del Responsabile della protezione dei dati, si riscontri la possibilità di migliorare ulteriormente il trattamento dei dati effettuato dai vari uffici comunali nell'ottica di obiettivi di efficienza, il Responsabile del trattamento procede nel riesame e nella sostituzione delle misure già applicate.

3. La notifica al Garante deve presentare il seguente contenuto minimo:

- la natura della violazione dei dati personali le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del Comune per porre rimedio alla violazione dei dati personali.

A questo contenuto minimo è possibile aggiungere ogni altra informazione che il Titolare ritiene necessaria.

4. In caso non si sia in possesso delle informazioni di cui al comma 3 il Titolare procederà a comunicare entro 72 ore quelle di cui è a conoscenza e successivamente, appena verrà in possesso dei dati mancanti effettuerà una comunicazione integrativa senza ingiustificato ritardo.

5. Il Garante può indicare l'adozione di misure integrative a quelle già descritte nella notifica, oltre che fornire osservazioni per porre rimedio alla violazione e può anche imporre la comunicazione all'interessato di cui al successivo articolo, qualora non sia stata ritenuta necessaria dal Comune.

### ***Art. 37 - Comunicazione all'interessato***

1. Il Titolare del trattamento comunica, senza giustificato ritardo, all'interessato la violazione in presenza solo di rischio elevato per i diritti e le libertà delle persone fisiche. Quanto più attuale è il dato violato tanto maggiore è la probabilità di rischio elevato, intendendosi per attualità il tempo trascorso dall'acquisizione del dato.

2. La comunicazione all'interessato va effettuata con un linguaggio semplice e chiaro e deve presentare anch'essa un contenuto minimo rappresentato da:

- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali

3. In caso non ricorrano i presupposti per la notifica al Garante come indicati dall'articolo precedente, non si procede nemmeno alla comunicazione all'interessato.

Questa inoltre non è necessaria se:

- i dati violati erano soggetti a misure di protezione tali da renderli incomprensibili, perché per es. sottoposti a cifratura;
- 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;
- la comunicazione ad personam richiederebbe sforzi sproporzionati per l'elevato numero di interessati. In tal caso, il Comune può procedere ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analogo efficacia; es. tramite web o giornale locale.

#### ***Art. 41 - Trattamento illecito dei dati***

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione delle norme sulla protezione dei dati personali, è punito, se dal fatto deriva documento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione delle norme sulla materia è punito, se dal fatto deriva documento, con la reclusione da uno a tre anni e la pena accessoria della pubblicazione della sentenza ai sensi degli artt. 167 e 172, D.Lgs. n. 196/2003.

#### ***Art. 42 - Falsità nelle dichiarazioni e notificazioni al Garante della privacy***

I Responsabili di settore o il Responsabile della protezione dei dati (DPO) che in esecuzione delle rispettive competenze procedono per conto del Comune con notificazioni, comunicazioni al Garante, qualora forniscano false dichiarazioni o attestazioni o producono documenti falsi, salvo che il fatto costituisca reato più grave, sono puniti con la reclusione da sei mesi a tre anni e la pena accessoria della pubblicazione della sentenza ai sensi degli artt. 168 e 172, D.Lgs. n. 196/2003.

#### ***Art. 43 - Omessa predisposizione di misure di sicurezza***

Il Titolare del trattamento e le persone fisiche che agiscono per suo conto che non adottino le misure di sicurezza minime sono penalmente responsabili e sono puniti con arresto fino a due anni dalle autorità giudiziarie competenti, oltre con la pena accessoria della pubblicazione della sentenza ai sensi degli artt.169 e 172, D.Lgs. n. 196/2003.

### **TITOLO VIII - ENTRATA IN VIGORE**

#### ***Art. 44 - Abrogazioni***

1. Il presente regolamento sostituisce il precedente adottato prima dell'entrata in vigore del Regolamento UE 679/2016; per quanto non previsto si applicano direttamente le norme del regolamento europeo.
2. Il presente regolamento fa riferimento alle sole norme del Codice della privacy ancora oggi vigenti.

#### ***Art. 45 - Entrata in vigore del regolamento***

1. Il presente regolamento entra in vigore il quindicesimo giorno successivo alla data di pubblicazione.
2. Il regolamento e la relativa modulistica per l'esercizio dei diritti sono resi pubblici mediante pubblicazione sul sito internet del Comune, nella Sezione Amministrazione Trasparente.
3. Copia del regolamento va inoltrata al Segretario comunale, ai responsabili di settore ed al DPO, ed ogni altro dipendente che tratta dati personali nel Comune.