APPROVATO CON DELIBERA DI CONSIGLIO COMUNALE N. 36 DEL 05-07-2019

# REGOLAMENTO PER L'IMPLEMENTAZIONE DI MISURE ORGANIZZATIVE E PROCESSI INTERNI SULLA PROTEZIONE DEI DATI PERSONALI IN ATTUAZIONE DEL REGOLAMENTO (UE) 679/2016 E DEL D.LGS. N. 101/2018.


**TITOLO I – DISPOSIZIONI GENERALI E PRINCIPI**

*Articolo 1 – OGGETTO*

*Articolo 2 – DEFINIZIONI*

*Articolo 3 – QUADRO NORMATIVO DI RIFERIMENTO*

*Articolo 4 – FINALITÀ*

*Articolo 5 – PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI*

**TITOLO II – IL TRATTAMENTO DEI DATI PERSONALI**

*Articolo 6 – TRATTAMENTO DEI DATI PERSONALI, RICOGNIZIONE DEI TRATTAMENTI*

*Articolo 7 – TIPOLOGIE DI DATI TRATTATI*

*Articolo 8 – TRATTAMENTO DEI DATI PARTICOLARI E DEI DATI RELATIVI A CONDANNE PENALI E REATI*

*Articolo 9 – TRATTAMENTO DEI DATI DEL PERSONALE*

*Articolo 10 – REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO*

*Articolo 11 – REGISTRO DELLE CATEGORIE DI TRATTAMENTO*

*Articolo 12 – INFORMATIVA*

**TITOLO III – SOGGETTI**

*Articolo 13 – TITOLARE DEL TRATTAMENTO*

*Articolo 14 – RESPONSABILE DEL TRATTAMENTO E SUB-RESPONSABILE*

*Articolo 15 – AUTORIZZATI AL TRATTAMENTO*

*Articolo 16 – AMMINISTRATORE DI SISTEMA*

*Articolo 17 – RESPONSABILE DELLA PROTEZIONE DEI DATI*

**TITOLO IV – DIRITTI DEGLI INTERESSATI**

*Articolo 18 – DIRITTI DELL'INTERESSATO*

*Articolo 19 – DIRITTO DI ACCESSO*

*Articolo 20 – DIRITTO ALLA RETTIFICA*

*Articolo 21 – DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)*

*Articolo 22 – DIRITTO ALLA LIMITAZIONE*

*Articolo 23 – DIRITTO ALLA PORTABILITÀ*

*Articolo 24 – DIRITTO DI OPPOSIZIONE*

*Articolo 25 – MODALITÀ DI ESERCIZIO DEI DIRITTI DELL'INTERESSATO*

**TITOLO V – SICUREZZA DEI DATI PERSONALI**

*Articolo 26 – MISURE DI SICUREZZA*
*Articolo 27 – SENSIBILIZZAZIONE E FORMAZIONE*
*Articolo 28 – VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)*
*Articolo 29 – CONSULTAZIONE PREVENTIVA*
*Articolo 30 – VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)*
TITOLO VI – NORME TRANSITORIE E FINALI
*Articolo 31 – PIANO DI PROTEZIONE DEI DATI PERSONALI*
*Articolo 32 – DISPOSIZIONI FINALI*
*Articolo 33 – ENTRATA IN VIGORE*

## TITOLO I – DISPOSIZIONI GENERALI E PRINCIPI

### Articolo 1 – OGGETTO

1. Il presente Regolamento disciplina le misure organizzative, procedimentali, i processi interni di attuazione e le regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento Europeo n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati) e del d.lgs. n. 101/2018.

### Articolo 2 – DEFINIZIONI

1. Ai fini del presente regolamento si recepiscono le seguenti definizioni, enunciate dall'art. 4 del Regolamento UE 2016/679:
   a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
   b) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
   c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
   d) «**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;
   e) «**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;
   f) «**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;
   g) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
   h) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, o altro organismo che tratta dati personali per conto del titolare del trattamento;
   i) «**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 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;

j) «**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;

k) «**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;

l) «**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;

m) «**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;

n) «**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;

o) «**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;

p) «**stabilimento principale**»:

1) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

2) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

q) «**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;

r) «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

s) «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

t) «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

u) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

v) «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

1) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

2) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

3) un reclamo è stato proposto a tale autorità di controllo;

w) «**trattamento transfrontaliero**»:

1) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

2) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

x) «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

y) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

z) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

2. Ai fini del presente regolamento, inoltre, si intende per:
   - "**GDPR**": **G**eneral **D**ata **P**rotection **R**egulation, il Regolamento UE 2016/679;
   - "**DPO** o **RPD**": **D**ata **P**rotection **O**fficer, il **R**esponsabile della **P**rotezione dei **D**ati;
   - "**DPIA**": **D**ata **P**rotection **I**mpact **A**ssessment, la Valutazione d'impatto sulla protezione dei dati.

## Articolo 3 – QUADRO NORMATIVO DI RIFERIMENTO

1. Il presente Regolamento tiene conto dei seguenti documenti:
   - Regolamento UE 679/2016 (GDPR – General Data Protection Regulation) 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, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, in vigore dal 24 maggio 2016 ed applicabile a partire dal 25 maggio 2018 in via diretta in tutti i Paesi UE dal 25 maggio 2018
   - D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e ss.mm.ii.;
   - D.Lgs. 19 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati)". (GU Serie Generale n. 205 del 4 settembre 2018);
   - Linee-guida e pareri del Gruppo di Lavoro Articolo 29 sulla protezione dei dati (WP29);
   - Linee-guida, provvedimenti e raccomandazioni del Garante per la Protezione dei Dati Personali.

## Articolo 4 – FINALITÀ

1. I trattamenti sono compiuti dal Comune per le seguenti finalità:
   a) 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;
      - la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
      - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

b) adempimento di un obbligo legale al quale è soggetto il Comune;
c) esecuzione di un contratto con soggetti interessati per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

### Articolo 5 – PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

1. Per le finalità di cui all'articolo 4 del presente Regolamento, il Comune di SANT'ANGELO DI BROLO effettua il trattamento dei dati personali nel rispetto delle disposizioni del Regolamento UE 2016/679, dei diritti e libertà fondamentali delle persone fisiche, nonché del diritto alla riservatezza ed all'identità delle persone fisiche.
2. I dati personali sono:
   a) trattati in conformità alle norme di legge, cioè in modo lecito, corretto e trasparente;
   b) raccolti per finalità determinate, esplicite e legittime. Le finalità del trattamento devono essere predeterminate e chiare ed eventuali ulteriori trattamenti non devono avere finalità incompatibili con quella originaria. Un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o ai fini statistici non è considerato incompatibile con le finalità iniziali (limitazione della finalità);
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
   d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza);
   e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato (limitazione della conservazione);
   f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (integrità e riservatezza).
3. I diritti sui dati personali concernenti persone decedute, possono essere esercitati da chi agisce per la tutela del defunto o per motivi familiari meritevoli di tutela.
4. Il trattamento dei dati osserva il principio di responsabilizzazione che comporta non solo l'obbligo del rispetto delle norme ma anche quello di comprovarlo.

## TITOLO II – IL TRATTAMENTO DEI DATI PERSONALI

### Articolo 6 – TRATTAMENTO DEI DATI PERSONALI, RICOGNIZIONE DEI TRATTAMENTI

1. Il Titolare tratta i dati personali per lo svolgimento delle proprie finalità istituzionali, come identificate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal GDPR, dalle Linee Guida e dai provvedimenti del Garante.
2. Il Titolare effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:
   a) la gestione del personale dipendente, ivi comprese le procedure di assunzione;
   b) la gestione dei soggetti che intrattengono rapporti giuridici con il titolare, diversi dal rapporto di lavoro dipendente, e che operano a qualsiasi titolo all'interno della struttura organizzativa del titolare, ivi compresi gli stagisti, tirocinanti e i volontari;
   c) la gestione dei rapporti con i consulenti, i libero-professionisti, i fornitori per l'approvvigionamento di beni e di servizi nonché con le imprese per l'esecuzione lavori, opere e di interventi di manutenzione;
   d) la gestione dei rapporti con i soggetti accreditati o convenzionati per i servizi socio-assistenziali;

e) la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.

3. Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del Titolare, da parte degli uffici competenti, dai responsabili del trattamento, dai sub responsabili - i soggetti responsabili del procedimento al quale è sotteso il trattamento dati – dagli incaricati e/o autorizzati.
4. Ai fini del trattamento, il Titolare provvede, per il tramite degli uffici, alla integrale ricognizione e all'aggiornamento di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti del titolare medesimo, funzionali alla formazione del Registro delle Attività di Trattamento. È compito dei Responsabili del processo di trattamento dei dati effettuare e documentare l'aggiornamento periodico, almeno annuale, della ricognizione dei trattamenti e del relativo Registro, e la valutazione periodica, semestrale, del rispetto dei principi di cui all'art. 5 del presente Regolamento con riferimento a tutti i trattamenti inclusi nell'indice.
5. Il Titolare, i responsabili del trattamento, i sub responsabili del processo di trattamento dei dati e gli incaricati e/o autorizzati si attengono alle modalità di trattamento indicate nel GDPR, nonché nelle disposizioni attuative e nelle Linee guida del Garante per la protezione dei dati personali.

## Articolo 7 – TIPOLOGIE DI DATI TRATTATI

1. Nell'ambito dei trattamenti inclusi nell'indice dei trattamenti, il Titolare, nell'esercizio delle sue funzioni istituzionali, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:
   a) dati comuni: elementi di identificazione personale (nome e cognome, luogo e data di nascita, ecc.); numeri di identificazione personale (codice fiscale, n. carta d'identità, ecc.); informazioni su Stato Civile e famiglia (nominativo moglie, figli, appartenenti al nucleo familiare, ecc.); informazioni sul lavoro (occupazione, qualifiche professionali, ecc.); informazioni su istruzione e cultura (titolo di studio, curriculum, ecc.); informazioni economiche-finanziarie (proprietà, redditi, mutui, ecc.);
   b) dati particolari: i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
   c) dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

## Articolo 8 – TRATTAMENTO DEI DATI PARTICOLARI E DEI DATI RELATIVI A CONDANNE PENALI E REATI

1. Il Titolare effettua il trattamento dei dati particolari per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, secondo modalità volte a rispettare l'essenza del diritto alla protezione dei dati e prevedendo misure appropriate e specifiche per prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

## Articolo 9 – TRATTAMENTO DEI DATI DEL PERSONALE

1. Il Titolare tratta i dati, anche particolari e relativi alle condanne penali e ai reati, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo. Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.
2. Il Titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica. Il trattamento dei dati particolari del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati

personali, e quando non si possa prescindere dall'utilizzo di tali dati, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.

3. La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando diciture generiche o codici numerici. Non sono infatti ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile.
4. Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

## Articolo 10 – REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

1. Il Titolare del trattamento istituisce un registro, in forma scritta, delle attività di trattamento svolte sotto la propria responsabilità.
2. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto del Titolare del trattamento, eventualmente del Contitolare del trattamento, del Responsabile della Protezione dei Dati;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
3. Il Registro è tenuto dal Titolare presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.
4. Il Registro deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo.

## Articolo 11 – REGISTRO DELLE CATEGORIE DI TRATTAMENTO

1. Il Responsabile del trattamento tiene un registro di tutte le categorie di attività relative al trattamento svolte per conto di un Titolare del trattamento.
2. Il Registro delle categorie di attività trattate da ciascun Responsabile, reca le seguenti informazioni:
   a) il nome ed i dati di contatto del Titolare del trattamento, eventualmente del Contitolare del trattamento, del Responsabile della Protezione dei Dati e del Responsabile del trattamento;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
3. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea.
4. Il Registro deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo.

## Articolo 12 – INFORMATIVA

1. Il Titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dal GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

2. L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.
3. L'informativa è fornita, mediante idonei strumenti cui:
   a) appositi moduli da consegnare agli interessati ove sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
   b) avvisi agevolmente visibili dal pubblico posti nei locali di accesso delle strutture del Titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
   c) apposita avvertenza inserita nelle comunicazioni, nei contratti ovvero nelle lettere di affidamento di incarichi al personale dipendente, ai soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, ai tirocinanti, ai volontari, agli stagisti ed altri soggetti che entrano in rapporto con il Titolare;
   d) resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'autorizzato al trattamento dei dati relativi alle procedure.
4. L'informativa contiene il seguente contenuto minimo:
   a) l'identità e i dati di contatto del titolare;
   b) i dati di contatto del RPD/DPO;
   c) le finalità del trattamento;
   d) i destinatari dei dati;
   e) la base giuridica del trattamento;
   f) se il titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
   g) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
   h) i diritti dell'interessato previsti dal GDPR;
   i) il diritto di presentare un reclamo all'autorità di controllo;
   j) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.
5. Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve contenere altresì:
   a) le categorie di dati personali trattati;
   b) la fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico.
6. L'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.
7. Apposite informative devono essere inserite nei seguenti documenti: bandi e documentazione di affidamento dei contratti pubblici, contratti, accordi o convenzioni, bandi di concorso pubblico, segnalazioni di disservizio e, più in generale, in ogni altro documento contenente dati personali.

## TITOLO III – SOGGETTI

### Articolo 13 – TITOLARE DEL TRATTAMENTO

1. Il Titolare del trattamento è il soggetto cui competono le decisioni in ordine alle finalità, alle modalità di trattamento di dati personali e strumenti utilizzati.
2. Il Comune di SANT'ANGELO DI BROLO, rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").
3. Il Titolare provvede a:
   a) definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento, provvedendo all'inserimento di tali obiettivi strategici nei documenti di programmazione e pianificazione, previa apposita analisi preventiva della situazione in essere, tenuto conto dei

costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche;

b) mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente al GDPR, al D. Lgs. 30 giugno 2003, n. 196, al D.Lgs. 19 agosto 2018, n. 101 e al presente Regolamento;

c) delegare ovvero a designare, con proprio atto, i Dirigenti/Responsabili P.O. delle singole aree/settori in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza, per i compiti, le funzioni e i poteri in ordine ai processi, procedimenti e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, impartendo ad essi, le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;

d) formare e aggiornare l'elenco dei dirigenti/P.O., delegati o designati, ed a pubblicarlo sul sito web istituzionale;

e) designare quali Responsabili del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali. La designazione del Responsabile viene effettuata mediante atto da parte del Titolare del trattamento da allegare agli accordi, convenzioni, contratti o incarichi professionali che prevedono l'affidamento di trattamenti di dati personali esternamente al Titolare. L'accettazione della nomina e l'impegno a rispettare le disposizioni del GDPR e del presente Regolamento sono condizioni necessarie per l'instaurarsi del rapporto giuridico fra le parti.

f) designare, con proprio atto, il Responsabile per la Protezione dei Dati personali;

g) effettuare, 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, una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento;

h) adottare misure appropriate per fornire all'interessato le informazioni indicate dagli artt. 13 e 14 RGPD;

i) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;

j) agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio;

k) favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;

l) favorire l'adesione a meccanismi di certificazione;

m) assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.

## Articolo 14 – RESPONSABILE DEL TRATTAMENTO E SUB-RESPONSABILE

1. Il Responsabile è il soggetto che agisce per conto del Titolare.
2. Il Responsabile è designato dal Titolare facoltativamente. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3. Il Titolare, in considerazione della complessità e della molteplicità delle funzioni istituzionali, può designare quali Responsabili del trattamento dei dati personali, unicamente i soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in

modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato (GDPR, art. 28).

4. Il Sindaco, nella qualità di Titolare del trattamento, designa, con proprio atto, i Responsabili del trattamento, uno per ogni area e/o settore dell'Ente.
5. I Responsabili del trattamento per il Comune devono avere la qualifica di Dirigenti/Responsabili P.O.;
6. I dipendenti del Comune, Responsabili del trattamento, sono designati, di norma, mediante decreto di designazione del Sindaco, nel quale sono tassativamente disciplinati:
   a) la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
   b) il tipo di dati personali oggetto di trattamento e le categorie di interessati;
   c) gli obblighi ed i diritti del Titolare del trattamento.
7. Le funzioni dei Responsabili del trattamento devono essere specificate nel provvedimento di designazione e devono assicurare, almeno, le seguenti attività:
   a) mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato;
   b) garantire che eventuali sub responsabili o comunque ogni altro soggetto autorizzato al trattamento si sia impegnato alla riservatezza, abbia un adeguato obbligo legale alla riservatezza e venga adeguatamente formato;
   c) tenere un registro delle categorie di attività di trattamento svolte per conto del Titolare;
   d) collaborare alle richieste di accesso, di limitazione ed opposizione degli interessati relativi a trattamenti di dati personali;
   e) assistere il Titolare nella conduzione della "DPIA" fornendo allo stesso ogni informazione di cui è in possesso;
   f) fornire ogni informazione al Responsabile della Protezione dei Dati ogni qualvolta debbono essere assunte decisioni che impattano sulla protezione dei dati e consultarlo con immediatezza qualora si verifichi una violazione dei dati o un altro incidente;
   g) trattare i dati seguendo le istruzioni e le normative in materia garantendone la riservatezza;
   h) garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione e si sia impegnato alla riservatezza;
   i) sensibilizzare e formare il personale che partecipa ai trattamenti ed alle connesse attività di controllo;
   j) informare immediatamente il Titolare, della conoscenza di casi di violazione dei dati personali (c.d. "data breach") per l'eventuale successiva notifica della violazione al Garante per la Protezione dei Dati Personali..
8. Il Titolare può avvalersi, per il trattamento dei dati personali, anche "particolari", di soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali, designandoli con atti giuridici in forma scritta, che specifichino 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.
9. È consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per le specifiche attività di trattamento nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario.

## Articolo 15 – AUTORIZZATI AL TRATTAMENTO

1. Gli autorizzati al trattamento sono le persone fisiche, dipendenti del Titolare, designati da ciascun Dirigente/Responsabile P.O., incaricati di svolgere le operazioni di trattamento dei dati personali di competenza con l'indicazione specifica dei compiti, dell'ambito di trattamento consentito, e delle modalità.
2. La designazione dell'autorizzato al trattamento dei dati personali è di competenza del Dirigente/Responsabile P.O.; la nomina è effettuata per iscritto e individua specificatamente i compiti spettanti all'autorizzato e le modalità cui deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito.

3. A prescindere dalla nomina, si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale risulti individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima. Per effetto di tale disposizione, ogni dipendente preposto ad un determinato servizio/ufficio, tenuto ad effettuare operazioni di trattamento nell'ambito di tale servizio, è da considerare, "autorizzato".
4. Gli autorizzati devono comunque ricevere idonee ed analitiche istruzioni, anche per gruppi omogenei di funzioni, riguardo le attività sui dati affidate e gli adempimenti a cui sono tenuti.
5. Gli autorizzati collaborano con il Titolare ed il Dirigente/Responsabile P.O. segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.
6. In particolare, gli autorizzati devono assicurare che, nel corso del trattamento, i dati siano:
   a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
   b) raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
   d) esatti e, se necessario, aggiornati;
   e) devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
   f) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;
   g) trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.
7. Gli autorizzati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e dal Dirigente/Responsabile P.O., nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del Titolare.
8. Tutti i soggetti che svolgono un'attività di trattamento dei dati, e che non sono dipendenti del Titolare, quali a titolo meramente esemplificativo i tirocinanti, i volontari e i soggetti che operano temporaneamente all'interno della struttura organizzativa del Titolare, devono essere autorizzati al trattamento tramite atto scritto di nomina. Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli autorizzati dipendenti del Titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
9. Gli autorizzati operano sotto la diretta responsabilità del Responsabile che li ha nominati, al quale rispondono.

## Articolo 16 – AMMINISTRATORE DI SISTEMA

1. L'amministratore di sistema sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione.
2. La designazione dell'amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza.
3. La designazione dell'amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
4. L'amministratore di sistema svolge attività, quali: il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.
5. Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono essere complete, inalterabili, verificabili nella loro integrità ed adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.

6. Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato, con cadenza annuale, da parte del titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.

## Articolo 17 – RESPONSABILE DELLA PROTEZIONE DEI DATI

1. Il Titolare del trattamento dei dati nomina, con proprio provvedimento, il Responsabile della Protezione dei dati tra i dirigenti dell'Ente esperti in materia di disciplina della protezione dei dati e della prassi in materia, oppure può affidare le funzioni di Responsabile della protezione dei dati anche a soggetti esterni, esperti nella materia, selezionati con procedura ad evidenza pubblica. Il Responsabile così selezionato agirà in posizione di autonomia e non avrà ulteriori incarichi nell'Ente che possano dare adito a conflitto di interesse. Nel rispetto della normativa vigente in materia, le funzioni, le competenze, i rapporti, sono disciplinati con apposito contratto di servizio il cui contenuto deve essere conforme all'art. 39 del Regolamento UE 2016/679.
2. Il RPD 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 RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD 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 e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
   b) sorvegliare l'osservanza del RGPD 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 valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;
   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'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;
   f) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto d'interesse. L'assenza di tale conflitto è strettamente connessa agli obblighi di indipendenza del RPD.
3. Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   a) il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
   b) il RPD 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;
   c) il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;

d) il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

4. Nello svolgimento dei compiti affidatigli il RPD 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 RPD:
   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.
5. Il RPD 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.
6. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili (in relazione alle dimensioni organizzative del Comune):
   a) il Responsabile per la prevenzione della corruzione e per la trasparenza;
   b) il Responsabile del trattamento;
   c) qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
7. Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare, è assicurato al RPD:
   a) 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 (DUP), di bilancio, di Peg e di Piano della performance;
   b) tempo sufficiente per l'espletamento dei compiti affidati al RPD;
   c) supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero (in relazione alle dimensioni organizzative dell'Ente) tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale);
   d) 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;
   e) accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.
8. Il RPD 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 a una specifica questione attinente alla normativa in materia di protezione dei dati. Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.
9. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - od al Responsabile del trattamento.
10. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

## TITOLO IV – DIRITTI DEGLI INTERESSATI

### Articolo 18 – DIRITTI DELL'INTERESSATO

1. Il Titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, di seguito elencati, in conformità alla disciplina contenuta nel GDPR.

### Articolo 19 – DIRITTO DI ACCESSO

1. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di accesso secondo la quale l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
   a) le finalità del trattamento;
   b) le categorie di dati personali in questione;
   c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di Paesi terzi o organizzazioni internazionali;
   d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   e) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
   f) il diritto di proporre reclamo a un'autorità di controllo;
   g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
   h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.
3. Il Titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
4. Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

## Articolo 20 – DIRITTO ALLA RETTIFICA

1. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di rettifica, secondo la quale l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.
2. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
3. Il Titolare comunica a ciascuno dei destinatari, cui sono stati trasmessi i dati personali, le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

## Articolo 21 – DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

1. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di cancellazione («diritto all'oblio»), consistente nel diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:
   a) per l'esercizio del diritto alla libertà di espressione e di informazione;
   b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
   c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 GDPR;
   d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 GDPR, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
   e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Nel caso che i dati siano stati diffusi pubblicamente, anche su siti web, il Titolare del trattamento, tenendo conto dei costi di attuazione, è tenuto ad informare gli altri titolari che trattano i medesimi dati, della richiesta di cancellazione degli stessi, salvo che ciò non sia possibile o richieda uno sforzo sproporzionato.

## Articolo 22 – DIRITTO ALLA LIMITAZIONE

1. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto alla limitazione, consistente nel diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle seguenti condizioni:
   a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza di tali dati personali;
   b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
   c) benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   d) l'interessato si è opposto al trattamento ai sensi dell'articolo21, paragrafo 1 GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.
2. Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18 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.
3. L'interessato, che ha ottenuto la limitazione del trattamento, è informato dal Titolare prima che detta limitazione sia revocata.
4. Il Titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

## Articolo 23 – DIRITTO ALLA PORTABILITÀ

1. Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del GDPR, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

## Articolo 24 – DIRITTO DI OPPOSIZIONE

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione sulla base di tali disposizioni.
2. Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali, salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Il diritto di cui ai paragrafi 1 e 2 dell'art. 21 GDPR è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
3. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 del GDPR, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

## Articolo 25 – MODALITÀ DI ESERCIZIO DEI DIRITTI DELL'INTERESSATO

1. Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del GDPR e del presente Regolamento.
2. La richiesta per l'esercizio dei diritti può essere fatta pervenire:
   a) direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso, come ad esempio, la conoscenza personale;
   b) tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;
   c) tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;
   d) in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;
   e) dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una
   f) persona giuridica, un ente o un'associazione.
3. L'interessato può presentare o inviare la richiesta di esercizio dei diritti:
   a) al Titolare o Responsabile del trattamento, che conserva e gestisce i dati personali dell'interessato;
   b) all'ufficio protocollo generale del Titolare o all'ufficio per le relazioni con il pubblico.
4. La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.
5. Fermo restando l'accesso ai dati personali, il Titolare autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso.
6. All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa. I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.
7. L'accesso dell'interessato ai propri dati personali: può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del Titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.

## TITOLO V – SICUREZZA DEI DATI PERSONALI

### Articolo 26 – MISURE DI SICUREZZA

1. Il Titolare, nel trattamento dei dati personali, garantisce l'applicazione di misure idonee a soddisfare la protezione dei dati fin dalla progettazione, ovvero 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 dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
2. In particolare, il Titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate a garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono almeno:
   a) la pseudonimizzazione e la cifratura dei dati personali trattati;
   b) procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   c) modalità per garantire il ripristino tempestivo nell'accesso ai 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.

## Articolo 27 – SENSIBILIZZAZIONE E FORMAZIONE

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio. A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale e l'attività informativa diretta a tutti coloro che hanno rapporti con il Titolare.
2. Per garantire la conoscenza capillare delle disposizioni del presente Regolamento, al momento dell'ingresso in servizio è data a ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale, con i riferimenti per l'acquisizione del presente Regolamento, pubblicato sul sito istituzionale.
3. Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni.
4. Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, anche integrati con gli interventi di formazione anticorruzione, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.
5. La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il titolare.
6. La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

## Articolo 28 – VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

1. La valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
2. 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, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
3. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.
4. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti 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;
   b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

5. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.
   Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.
   Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
   L'Amministratore di Sistema, se nominato, e/o l'ufficio competente dei sistemi informativi, forniscono supporto al Titolare per lo svolgimento della DPIA.
6. Il RPD può proporre lo svolgimento di una DPIA 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.
7. La DPIA non è necessaria nei casi seguenti:
   a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
   b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
   c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
   d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

   Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica.
8. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
   a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei

dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
   - delle finalità specifiche, esplicite e legittime;
   - della liceità del trattamento;
   - dei dati adeguati, pertinenti e limitati a quanto necessario;
   - del periodo limitato di conservazione;
   - delle informazioni fornite agli interessati;
   - del diritto di accesso e portabilità dei dati;
   - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
   - dei rapporti con i responsabili del trattamento;
   - delle garanzie per i trasferimenti internazionali di dati;
   - consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

9. Il Titolare 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.
10. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche 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.
11. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

## Articolo 29 – CONSULTAZIONE PREVENTIVA

1. Il Titolare, prima di procedere al trattamento dei dati, consulta, per il tramite del RPD/PDO, il Garante qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate.

## Articolo 30 – VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

1. Per violazione dei dati personali (data breach) si intende 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 Comune.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
   a) danni fisici, materiali o immateriali alle persone fisiche;
   b) perdita del controllo dei dati personali;

c) limitazione dei diritti, discriminazione;
d) furto o usurpazione d'identità;
e) perdite finanziarie, danno economico o sociale;
f) decifratura non autorizzata della pseudonimizzazione;
g) pregiudizio alla reputazione;
h) perdita di riservatezza dei dati personali protetti da segreto professionale.

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare 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. 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 (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
   - comportare rischi imminenti e con un'elevata probabilità di accadimento (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 (ad esempio utenti deboli, minori, soggetti indagati).
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle 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 Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

## TITOLO VI – NORME TRANSITORIE E FINALI

### Articolo 31 – PIANO DI PROTEZIONE DEI DATI PERSONALI

1. Al fine di fornire tutte le istruzioni utili per un'efficace implementazione di un sistema strutturato di gestione della protezione dei dati personali, in attuazione alle disposizioni europee, nazionali, al presente regolamento e alle linee guida del Garante, il Comune si dota di un apposito piano.
2. Il piano di protezione dei dati personali deve fornire tutte le indicazioni, istruzioni e modulistica per creare il sistema di gestione del trattamento dei dati nell'ente locale e per tenerlo aggiornato.
3. In particolare, deve almeno disciplinare:
   a) Il Registro delle Attività di Trattamento e i Registri delle categorie di trattamento dei singoli Responsabili del trattamento;
   b) l'approccio metodologico della valutazione dei rischi e la DPIA;
   c) un apposito piano formativo che deve confluire nel più generale piano triennale della formazione dell'ente;
   d) le procedure per gli audit e i monitoraggi periodici;
   e) la modulistica per l'esercizio dei diritti degli interessati;
   f) la modulistica per la comunicazione con il Garante con particolare riferimento ai casi di Data breach;
   g) ogni altra direttiva, istruzione, indicazione utile ad un'efficace gestione del sistema della Privacy nell'Ente.

### Articolo 32 – DISPOSIZIONI FINALI

1. Per quanto non previsto nel presente Regolamento si applicano le disposizioni del GDPR e tutte le sue norme attuative vigenti.
2. Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.

## Articolo 33 – ENTRATA IN VIGORE

1. Il presente Regolamento entra in vigore il giorno in cui diviene esecutiva la relativa delibera di approvazione. Dalla stessa data cessano gli effetti delle disposizioni contenute su atti normativi interni dell'Ente adottati antecedentemente al presente regolamento in materia di privacy.
2. Il Regolamento è reso pubblico mediante pubblicazione sul sito web istituzionale del Comune, nella sezione Amministrazione Trasparente.