COMUNE DI VOLPIANO

Città Metropolitana di Torino

REGOLAMENTO PER LA CORRETTA GESTIONE E LA TUTELA DELLA RISERVATEZZA DEI DATI PERSONALI

Approvato con deliberazione del Consiglio Comunale n. 21 del 27.04.2026

Indice

Capo I – Disposizioni generali e principi

Articolo 1 – Oggetto del Regolamento

1. Il presente Regolamento disciplina le misure procedimentali e le regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo n. 679 del 27 aprile 2016 "Regolamento generale sulla protezione dei dati" (GDPR), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali nonché alla libera circolazione di tali dati.
2. Per quanto non previsto nel presente regolamento si rinvia al predetto Regolamento europeo 2016/679, alle vigenti fonti di diritto europee e nazionali, alle linee guida e ai provvedimenti del "Gruppo di Lavoro 29" nonché del Garante della Privacy e dell'EDPB (European Data Protection Board) alle direttive impartite dal Titolare del trattamento, dall'Amministratore del sistema informatico e dal Responsabile della protezione dei dati (DPO).

Articolo 2 - Definizioni

1. Ai fini del presente regolamento si intende per:
   - **Comune**: il Comune, nella qualità il titolare del trattamento dei dati personali, le cui funzioni sono esercitate dai propri organi di governo nell'ambito delle rispettive competenze;
   - **Garante**: l'Autorità di controllo ossia il Garante della Privacy;
   - **GDPR o REG. UE 2016/679**: il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "Regolamento generale sulla protezione dei dati";
   - **Codice**: il D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali";
   - **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile. 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;
   - **Dati particolari** (ex dati sensibili): i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
   - **Dati giudiziari**: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
   - **Dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
   - **Dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
   - **Dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
   - **Interessato**: la persona fisica titolare dei dati personali oggetto di trattamento;
   - **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;
   - **Limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
   - **Profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare

per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- **Pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **Archivio**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; 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;
- **Contitolari del trattamento**: due o più titolari del trattamento che determinano congiuntamente, mediante un accordo interno, le finalità e i mezzi del trattamento;
- **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **Sub-responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali a cui fa ricorso il responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;
- **Designato del trattamento**: Responsabile di Elevata Qualificazione dei singoli Uffici e strutture in cui si articola l'organizzazione comunale, preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;
- **Persona autorizzata al trattamento**: persona fisica (dipendente, collaboratore) che, agendo sotto l'autorità del titolare del trattamento, abbia accesso a dati personali essendo stato autorizzato al loro trattamento;
- **DPO o Responsabile della protezione dei dati**: la persona fisica o giuridica che svolge i compiti di cui all'art. 39 del REG. UE 2016/679 o ulteriori compiti affidati dal titolare del trattamento sulla base di un contratto di servizi;
- **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 del trattamento;
- **Destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione 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;
- **Consenso dell'interessato**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **Violazione dei dati personali**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **Unione**: l'Unione Europea;
- **Stato**: lo Stato italiano.

2. Per le definizioni non riportate nel precedente comma si rinvia all'elenco definizioni previste dall'art. 4 del GDPR.

Articolo 3 - Finalità

1. Il titolare garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.
2. Il titolare, nell'ambito delle sue funzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale.
3. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi, inclusi i procedimenti amministrativi di competenza del titolare, vanno gestiti conformemente alle disposizioni del Codice, del GDPR, e del presente Regolamento.

Articolo 4 – Principi applicabili al Trattamento (Rif. art. 5 – GDPR)

1. I dati personali sono trattati nel rispetto dei principi di:
   a) «liceità, correttezza e trasparenza»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
   b) «limitazione delle finalità»: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, prf. 1 del GDPR, considerato incompatibile con le finalità iniziali;
   c) «minimizzazione dei dati»: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
   d) «esattezza»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
   e) «limitazione della conservazione»: i dati personali sono 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, conformemente all'art. 89.1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;
   f) «integrità e riservatezza»: i dati personali sono 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 accidentali;
   g) «accountabitlity»: o responsabilizzazione, il titolare del trattamento è competente per il rispetto dei principi di cui al presente comma e deve essere in grado di comprovarlo.
2. Nelle ipotesi in cui disposizioni legislative, regolamentari o statutarie prevedano pubblicazioni obbligatorie, il responsabile del procedimento adotta le opportune misure atte a garantire la riservatezza dei dati personali a norma del GDPR, del "Codice della privacy" di cui al d.lgs. 30 giugno 2003. n.196, del "Codice della trasparenza" di cui al d.lgs. 14 marzo 2013, n. 33 e ss.mm.ii., delle norme di tempo in tempo vigenti, e dei provvedimenti del Garante della Privacy.

Articolo 5 – Liceità del trattamento (Rif. art. 6 – GDPR)

1. Il trattamento dei dati personali effettuato da questo Comune è lecito soltanto per lo svolgimento le proprie funzioni istituzionali e se:
   a) l'interessato ha espresso il consenso al trattamento dei suoi dati personali per una o più specifiche finalità: tale condizione si applica alle pubbliche amministrazioni soltanto allorché le stesse dovessero svolgere trattamenti non attinenti ai propri compiti istituzionali di interesse pubblico o all'esercizio dei

pubblici poteri attribuiti dal diritto dell'Unione o dello Stato;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso interessato;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto questo Comune; a tal fine lo Stato membro può mantenere o introdurre disposizioni più specifiche riguardo al trattamento, determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui agli articoli da 85 a 91 del GDPR. (art. 6, prf. 2, GDPR)
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, se non trova applicazione alcuna delle altre predette condizioni;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito questo Comune; a tal fine lo Stato membro può mantenere o introdurre disposizioni più specifiche riguardo al trattamento, determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui agli articoli da 85 a 91 del GDPR. (art. 6, prf. 2, GDPR)
f) La base su cui si fonda il trattamento dei dati di cui alle lettere c) ed e) del comma 1 deve essere stabilita dal diritto dell'Unione o dello Stato; rientrano in questo ambito i trattamenti dei dati personali 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 o regionale o provinciale trasferite o delegate o comunque affidate al Comune in base alla vigente legislazione.

2. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui alla lettera e) del comma 1, è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del GDPR, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX dello stesso GDPR .

3. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o dello Stato, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:
   a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
   b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
   c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9 del GDPR, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del GDPR;
   d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
   e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 6 – Consenso dell'interessato (Rif. Art. 7 GDPR)

1. Il Comune non deve richiedere agli interessati il consenso per il trattamento dei loro dati personali allorquando il trattamento dei dati è effettuato nello svolgimento dei propri compiti istituzionali di interesse

pubblico o connesso all'esercizio di pubblici poteri di cui è investito dal diritto dell'Unione o dello Stato.

2. Nelle fattispecie diverse da quelle di cui al precedente comma 1, qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Articolo 7 – Trattamento delle particolari categorie di dati (Rif. Art. 9 GDPR)

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il divieto di cui al precedente comma non si applica se si verifica uno dei seguenti casi:
   a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al comma 1;
   b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
   c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
   e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
   f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
   g) Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
   h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al comma 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, del GDPR sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al comma 1 possono essere trattati per le finalità di cui al comma 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o dello Stato o alle norme stabilite dagli organismi nazionali competenti.

Articolo 8 – Trattamento dei dati giudiziari (Rif. Art. 10 GDPR)

1. Il titolare conforma il trattamento delle particolari categorie di dati e dei giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.
2. Il titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento di particolari categorie di dati e dati giudiziari.

Capo II – Diritti dell'interessato

Articolo 9 – Informativa, comunicazione e modalità trasparenti per l'esercizio dei diritti dell'interessato (Rif. Art. 12 GDPR)

1. Il Comune adotta misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

2. Il Comune agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 12 a 18. Nei casi di cui all'articolo 11, paragrafo 2, del GDPR il Comune non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 12 a 18, salvo che il Comune dimostri che non è in grado di identificare l'interessato.

3. Il Comune fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 12 a 18 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il Comune informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato. Se non ottempera alla richiesta dell'interessato, il Comune informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

4. Le informazioni fornite ai sensi degli articoli 10 e 11 ed eventuali comunicazioni e azioni intraprese ai sensi

degli articoli da 12 a 18 e dell'articolo 29 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) rifiutare di soddisfare la richiesta. Incombe al Comune l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

5. Fatto salvo l'articolo 11 del GDPR, qualora il Comune nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 12 a 17, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

6. Le informazioni da fornire agli interessati a norma degli articoli 10 e 11 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

Articolo 10 – Informativa per i dati da raccogliere presso l'interessato (Rif. Art. 13 GDPR)

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il Comune fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
   a) l'identità e i dati di contatto del titolare del trattamento;
   b) i dati di contatto del DPO-responsabile della protezione dei dati;
   c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
   d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il Comune fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
   a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   c) qualora il trattamento di dati personali sia basato sul consenso espresso dall'interessato per una o più specifiche finalità oppure il trattamento delle particolari categorie di dati sia basato sul consenso espresso dall'interessato per una o più specifiche finalità e il diritto dell'Unione o dello Stato abbia disposto l'irrevocabilità del divieto di trattare gli stessi dati sensibili previsto dal paragrafo 1 dell'articolo 9 del GDPR , l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   d) il diritto di proporre reclamo a un'autorità di controllo;
   e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
   f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Qualora il Comune intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al comma 2.

Articolo 11 – Informativa per i dati da ottenere da soggetti diversi dall'interessato (Rif. Art. 14 GDPR)

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:
   a) l'identità e i dati di contatto del Comune;
   b) i dati di contatto del DPO-responsabile della protezione dei dati;
   c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
   d) le categorie di dati personali in questione;
   e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.

2. Oltre alle informazioni di cui al comma 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
   a) il periodo di conservazione dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   b) l'esistenza del diritto dell'interessato di chiedere al Comune l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   c) qualora il trattamento di dati personali sia basato sul consenso espresso dall'interessato per una o più specifiche finalità oppure il trattamento delle particolari categorie di dati sia basato sul consenso espresso dall'interessato per una o più specifiche finalità e il diritto dell'Unione o dello Stato abbia disposto l'irrevocabilità del divieto di trattare gli stessi dati sensibili previsto dal paragrafo 1 dell'articolo 9 del GDPR, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   d) il diritto di proporre reclamo a un'autorità di controllo;
   e) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
   f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Il Comune fornisce le informazioni di cui ai commi 1 e 2:
   a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
   b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati.

4. Qualora il Comune intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al comma 2.

5. I commi da 1 a 4 non si applicano se e nella misura in cui:
   a) l'interessato dispone già delle informazioni;
   b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, del GDPR o nella misura in cui l'obbligo di cui al comma 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il Comune adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
   c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o dello Stato, compreso un obbligo di segretezza previsto per legge.

Articolo 12 – Diritto di accesso dell'interessato (Rif. art. 15 GDPR)

1. 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, del GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Articolo 13 – Diritto di rettifica e integrazione (Rif. artt. 16 e 19 GDPR)

1. L'interessato ha il diritto di ottenere dal Comune la rettifica dei suoi dati personali inesatti nonché, tenuto conto delle finalità del trattamento, l'integrazione dei suoi dati personali incompleti, anche fornendo una dichiarazione integrativa. L'istanza di rettifica o integrazione è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
2. Alla rettifica ovvero all'integrazione dei dati richiesta dall'interessato provvede, senza ritardo e comunque entro 10 giorni lavorativi dalla data di arrivo della predetta istanza, il Responsabile del procedimento amministrativo cui si riferiscono i dati da rettificare o integrare.
3. Dell'eseguita rettifica o integrazione ovvero della motivata inammissibilità è data tempestiva comunicazione all'interessato con raccomandata con avviso di ricevimento o con notifica a mani o tramite PEC.
4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Articolo 14 – Diritto alla cancellazione (diritto all'oblio) (Rif. artt. 17 e 19 GDPR)

1. L'interessato ha il diritto di ottenere dal Comune la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Comune ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
   b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), ovvero all'art. 9, prf. 2, lett. a), del GDPR e se non sussiste altro fondamento giuridico per il trattamento;
   c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, del GDPR e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2, del GDPR;
   d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato cui è soggetto il titolare del trattamento;

2. L'istanza è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.

3. Il Comune, se ha reso pubblici dati personali ed è obbligato, ai sensi del comma 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento, che stanno trattando i dati personali, della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

4. I commi 1 e 2 non si applicano 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, del GDPR;
   d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, del GDPR nella misura in cui il diritto di cui al comma 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
   e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

5. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali, la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Articolo 15 – Diritto di limitazione di trattamento (Rif. artt. 18 e 19 GDPR)

1. L'interessato ha il diritto di ottenere dal Comune la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
   a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Comune 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 Comune 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'articolo 21, paragrafo 1, del 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 comma 1, 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 dello Stato.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del comma 1 è informato dal Comune prima che detta limitazione sia revocata.

4. Il titolare del trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali, la limitazione del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato e, inoltre, dà comunicazione all'interessato di tali

destinatari qualora l'interessato lo richieda.

Articolo 16 – Diritto alla portabilità dei dati (Rif. art. 20 GDPR)

1. Il diritto alla portabilità dei dati di cui all'articolo 20 del GDPR non si applica ai trattamenti svolti dal Comune necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso ente.

Articolo 17 – Diritto di opposizione (Rif. art. 21 GDPR)

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 necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune, compresa la profilazione sulla base di tali disposizioni. Il Comune si astiene dal trattare ulteriormente i dati personali salvo che 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.

2. L'opposizione è formulata dall'interessato per iscritto ed è inviata al Comune anche per posta elettronica.

Articolo 18 – Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (Rif. art. 22 GDPR)

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2. Il comma 1 non si applica nel caso in cui la decisione:
   a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
   b) sia autorizzata dal diritto dell'Unione o dello Stato, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
   c) si basi sul consenso esplicito dell'interessato.

3. Nei casi di cui al comma 2, lettere a) e c), il Comune attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al comma 2 non si basano sulle categorie particolari di dati di cui all'articolo 9, paragrafo 1, del GDPR, a meno che non siano applicabili l'articolo 9, paragrafo 2, lettere a) o g), del GDPR, e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Capo III - Soggetti

Articolo 19 – Titolare del trattamento (Rif. art. 24 GDPR)

1. Il Comune di Volpiano è il titolare del trattamento dei dati personali raccolti in banche dati, informatiche o cartacee, gestite dagli uffici comunali. Per il trattamento di dati il Comune può avvalersi anche di soggetti pubblici o privati esterni tramite un contratto di servizio o altro atto giuridicamente valido nel quale sono specificati le finalità e le modalità del trattamento, le categorie di dati da trattare, le responsabilità e i doveri facenti carico al soggetto che svolgerà il trattamento, determinandone la qualifica di contitolare o

responsabile del trattamento.

2. Le funzioni attribuite al Comune dal diritto dell'Unione e dello Stato sono esercitate dai propri organi di governo (Consiglio comunale, Giunta comunale, Sindaco) nell'ambito delle rispettive competenze. Il Sindaco rappresenta il Comune nella qualità di titolare del trattamento.

3. Il Comune è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

4. Il Comune mette in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR.

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

6. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, 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.

7. Il Titolare adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
   8. 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 Comune deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell' art. 35, GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 31.

9. Il Comune provvede a:
   a) designare i Referenti del trattamento (Designati del Trattamento) nelle persone dei Responsabili di Elevata Qualificazione delle singole strutture 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;
   b) nominare le Persone Autorizzate
   c) nominare il DPO-Responsabile della protezione dei dati;
   d) nominare l'Amministratore del sistema informatico;
   e) diramare le direttive necessarie per l'applicazione delle disposizioni del GDPR e del presente regolamento, sentiti il DPO, il Segretario Generale, l'Amministratore del sistema informatico e i Designati del trattamento.

10. Nelle convenzioni, nelle concessioni, nei contratti, negli incarichi professionali o in altri strumenti giuridici consentiti dalla legge con cui è affidata a soggetti esterni al Comune la gestione di attività e/o servizi per conto di questa Amministrazione comunale, è prevista espressamente la nomina degli stessi soggetti affidatari quali responsabili del trattamento dei dati personali connessi alle attività istituzionali affidate. Qualora negli atti vigenti manchi tale previsione, dovrà essere effettuata un'opportuna operazione di adeguamento.

11. Il Comune favorirà l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di

categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Articolo 20 – Contitolari del Trattamento (Rif. art. 26 GDPR)

1. 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, allorché due o più titolari determinano congiuntamente e in modo trasparente, mediante accordo interno, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 GDPR.

2. L'accordo definisce le responsabilità di ciascun titolare in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa europea o statale specificatamente applicabile. Tale accordo può individuare un punto di contatto comune per gli interessati.

Articolo 21 – Responsabili del Trattamento (Rif. art. 28 GDPR)

1. Il Comune nelle operazioni di trattamento si può avvalere di soggetti esterni opportunamente nominati quali Responsabili del trattamento. La nomina avviene con apposito atto di nomina, nel quale sono tassativamente previsti:
   - la finalità del trattamento o dei trattamenti assegnati;
   - il tipo di dati personali oggetto di trattamento;
   - le categorie di interessati coinvolti;

2. Il Responsabile del trattamento deve essere in grado, di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui al successivo articolo 28, rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

3. Il Comune può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di Responsabili del trattamento, forniscano le garanzie di cui al comma 2, stipulando contratti, 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.

4. Gli atti che disciplinano il rapporto tra il Titolare del trattamento e il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, del GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

5. Ai Responsabili del trattamento è consentita la nomina di sub-responsabili del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare del trattamento e il Responsabile del trattamento primario, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Se il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile primario conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.

6. Le operazioni di trattamento possono essere effettuate solo da sub-responsabili o da incaricati che operano sotto la diretta autorità del Responsabile del trattamento, attenendosi alle istruzioni loro impartite per iscritto dallo stesso Responsabile, le quali istruzioni individuano specificatamente l'ambito del trattamento consentito.

7. Il Responsabile del trattamento risponde, anche dinanzi al Titolare del trattamento, dell'operato del sub-

responsabile del trattamento e degli incaricati del trattamento, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile e dell'incaricato del trattamento.

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

9. Il Responsabile del trattamento provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare del trattamento, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare deve provvedere:
   - a tenere aggiornato il registro delle categorie di attività di trattamento svolte per conto del Titolare;
   - ad adottare le misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti;
   - ad autorizzare i dipendenti appartenenti alla sua struttura ad accedere ai dati personali al fine di svolgere il trattamento afferente i rispettivi compiti istituzionali;
   - a sensibilizzare e formare il personale che partecipa ai trattamenti in materia di protezione dei dati personali, fornendo le istruzioni per il corretto trattamento dei dati personali, e a controllare che le attività di trattamento, con particolare riferimento alle operazioni di comunicazione e diffusione, svolte dagli incaricati, siano conformi alle norme del GDPR;
   - a collaborare con il Titolare al fine di definire la valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
   - a informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso in cui il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati;
   - ad adottare le misure necessarie per facilitare l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del GDPR;

Articolo 22 – Persone autorizzate o incaricati del Trattamento (Rif. art. 29 – GDPR)

1. Le Persone Autorizzate al trattamento sono persone fisiche interne al Comune – componenti degli organi di governo e di controllo, dirigenti, dipendenti comunali e soggetti che a vario titolo collaborano con l'Amministrazione (stagisti, collaboratori occasionali, volontari ecc.) – che hanno accesso a dati personali ovvero agiscano sotto l'autorità diretta del Titolare del trattamento.

2. Le Persone Autorizzate al trattamento non possono svolgere operazioni di trattamento dei dati personali se non sono istruite in tal senso dal Titolare del trattamento.

3. Tra le Persone Autorizzate sono individuate e nominate le Persone Autorizzate Referenti, ovvero quei soggetti che in virtù del ruolo organizzativo ricoperto collaborano al coordinamento delle attività di trattamento con il Titolare del trattamento e il Data Protection Officer.

4. I dipendenti comunali e collaboratori sono designati quali Persone Autorizzate al trattamento dei dati personali con atto di nomina del Referente per la struttura organizzativa (Titolare dell'Elevata Qualificazione) in cui sono inseriti gli stessi dipendenti; in tale documento sono fornite indicazioni per le attività di trattamento che possono essere formulate anche con rinvio al registro dei trattamenti. Tale atto deve essere notificato al dipendente interessato, il quale non può esimersi dalla sua accettazione e attuazione.

5. I dipendenti e collaboratori nominati Persone Autorizzate (Incaricati) operano sotto l'autorità del Titolare del trattamento, attenendosi alle istruzioni impartite per iscritto, con particolare riferimento alla custodia degli atti e documenti analogici e digitali contenenti particolari categorie di dati e giudiziari e alle relative misure di sicurezza.

6. Alle Persone Autorizzate compete, in relazione al trattamento dei dati personali provvedere:
   - al trattamento dei dati personali per lo svolgimento delle funzioni istituzionali del Comune, in conformità alle disposizioni del GDPR;
   - alla raccolta e registrazione per gli scopi inerenti all'attività istituzionale svolta da ciascuno;
   - alla verifica in ordine alla loro pertinenza, completezza e non eccedenza delle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare del trattamento;
   - alla conservazione, rispettando le misure di sicurezza predisposte al riguardo.

7. Per ogni operazione di trattamento è da garantire la massima riservatezza.

8. Nel caso di allontanamento anche temporaneo dalla propria postazione di lavoro, l'incaricato verifica che non vi sia possibilità per chiunque non sia autorizzato all'accesso ai dati di accedere alle banche-dati e/o ai dati personali per i quali è in corso un qualsiasi tipo di trattamento. Il flusso di dati tra Titolare del trattamento, Designati del trattamento, Persone Autorizzate, Amministratore del sistema informatico, il Responsabile della protezione dei dati, Segretario Generale, componenti degli organi di governo e di controllo interno non costituisce "comunicazione" in senso tecnico quale operazione di trattamento; ne consegue che tale flusso non è soggetto ai limiti previsti per tale operazione di trattamento.

Articolo 23 – Amministratore del Sistema Informatico

1. L'Amministratore di sistema, individuato nel Responsabile del Centro Elaborazione Dati, sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione.

2. La nomina 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. 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.

3. L'amministratore di sistema svolge attività, quali:
   - mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio
   - 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.

4. 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, e 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.

5. 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.

6. Il titolare di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

7. L'Amministratore di sistema è destinatario degli interventi di formazione di aggiornamento.

Articolo 24 - DPO (Responsabile della Protezione dei dati) (Rif. artt. 37-39 GDPR)

1. Il Comune si avvale obbligatoriamente di un DPO - Data Protection Officer (RPD - Responsabile della protezione dei dati), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.

2. Il Responsabile della Trasparenza provvede, tempestivamente, a che i dati identificativi e di contatto del Responsabile della protezione dei dati siano:
   - pubblicati nel sito web istituzionale dell'Ente;
   - comunicati al Garante della Privacy;
   - comunicati ai componenti degli organi di governo, a tutti i dirigenti e dipendenti comunali, ai componenti degli organi di controllo interni e all'Amministratore del Sistema Informatico.

3. Sino alla designazione del nuovo DPO si intende prorogata di diritto la designazione del Responsabile della protezione dei dati in carica al momento della predetta proclamazione. Tale proroga è valida anche a seguito della nomina di un Commissario che sostituisca tutti gli organi di governo dell'Ente, salvo che lo stesso Commissario non ritenga necessario designare un nuovo Responsabile della protezione dei dati ovvero sostituire il Responsabile in carica all'atto della sua nomina.

4. Nell'atto di designazione del soggetto interno all'Ente ovvero nel contratto di servizio relativi all'affidamento dell'incarico di DPO devono essere riportati i compiti che lo stesso è tenuto a svolgere, tra cui almeno i seguenti:
   a) **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 dello Stato relative alla protezione dei dati; in tal senso il DPO indica al Titolare del trattamento 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 GDPR, di altre disposizioni dell'Unione o dello Stato relative alla protezione dei dati** nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; 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;
   c) **sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;**
   d) **fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento** ai sensi dell'articolo 35 del GDPR; il Titolare del trattamento, in particolare, si consulta con il DPO 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 GDPR ;
   e) **cooperare con il Garante per la protezione dei dati personali** e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione.

7. Il Titolare del trattamento si assicura che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   - il DPO è invitato a partecipare alle riunioni di coordinamento dei Designati del Trattamento che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
   - il DPO deve ricevere tempestivamente, tramite posta elettronica, dal Titolare del trattamento tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da essere edotto sulla evoluzione della gestione in materia e da poter rendere una consulenza idonea;

- è obbligatorio richiedere il parere del DPO sulle decisioni che impattano sulla disciplina e sulla prassi da seguire nell'Ente in materia di protezione dei dati; qualora la decisione assunta determini condotte difformi dal parere del DPO, è necessario motivare specificamente tale decisione;

8. Il DPO è tenuto a manifestare il proprio parere in merito alle decisioni o ai provvedimenti o ai comportamenti incompatibili con il GDPR adottati o tenuti dai componenti degli organi di governo e di controllo nonché degli organi di gestione e dei dipendenti ogni qual volta ne venga a conoscenza, dandone comunicazione al Titolare del trattamento.

9. Il Titolare del trattamento e i Designati del Trattamento sostengono il DPO nell'esecuzione dei compiti di cui all'articolo 39 del GDPR, fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. In particolare è assicurato al DPO:
   - supporto attivo per lo svolgimento dei compiti da parte dei Responsabili del trattamento, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di PEG, di Piano della performance e di Piano della formazione;
   - supporto adeguato in termini di risorse strumentali (sede e attrezzature) e umane (dipendenti comunali) costituite in gruppo di lavoro che lo coadiuvi nell'espletamento dei suoi compiti;
   - accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

10. Gli interessati possono contattare direttamente il DPO per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

11. Il DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o dello Stato.

Articolo 25 – Comunicazione interna di documenti contenenti dati personali

1. La comunicazione di documenti amministrativi, secondo la definizione di cui all'art. 1, comma 1, lettera a) del DPR n. 445/2000, contenenti dati personali ai componenti degli organi di governo, ovvero all'interno della struttura organizzativa di questo Comune, per ragioni d'ufficio e nell'ambito delle specifiche competenze dei servizi, non è soggetta a limitazioni particolari, salvo quelle espressamente previste da leggi e regolamenti.

2. Il Designato del trattamento può tuttavia disporre, con adeguata motivazione, le misure necessarie per la protezione dei dati personali, qualora la comunicazione concerna particolari categorie di dati e/o dati giudiziari.

Articolo 26 – Utilizzo di dati da parte dei componenti degli organi di governo e di controllo interno

1. Il Sindaco, i Consiglieri comunali e gli Assessori nonché i componenti degli organi di controllo interno hanno diritto di accedere a documenti amministrativi detenuti da questo Comune, contenenti dati personali detenuti dall'Amministrazione comunale, nei limiti e con le modalità previsti dalle disposizioni di legge e di regolamenti.

2. Le notizie e le informazioni così acquisite devono essere utilizzate esclusivamente per le finalità pertinenti alle rispettive competenze, rispettando il divieto di divulgazione dei predetti documenti nonché l'obbligo della segretezza del loro contenuto.

Capo IV – Sicurezza dei dati personali

Articolo 27 – Misure per la sicurezza dei dati personali (Rif. art. 32 GDPR)

1. Il Titolare, i Designati del trattamento nonché l'Amministratore del sistema informatico e il DPO-Responsabile della protezione dei dati provvedono, per quanto di rispettiva competenza, all'adozione e alla dimostrazione di attuazione concreta di misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resistenza dei sistemi e dei servizi con cui sono trattati i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Titolare del trattamento:
   - sistemi di autenticazione, autorizzazione e protezione (antivirus; firewall; antintrusione; altro);
   - misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

4. La conformità del trattamento dei dati al GDPR in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati.

5. Il Titolare e i Designati del trattamento nonché l'Amministratore del sistema informatico e il DPO provvedono, per quanto di rispettiva competenza, a impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi e i dati di contatto del Titolare e del DPO sono pubblicati, a cura del Responsabile della Trasparenza, sul sito web istituzionale del Comune, sezione "Amministrazione trasparente".

7. I Designati del trattamento provvedono, nell'ambito di propria competenza, a effettuare periodiche verifiche sulla corretta applicazione della normativa in materia di trattamento dei dati personali nell'ambito delle articolazioni organizzative cui sono preposti, in accordo con i controlli specifici effettuati dal responsabile della protezione dei dati.

Articolo 28 – Registro unico della attività di trattamento dei dati personali (Rif. art. 30 GDPR)

1. Con deliberazione di Giunta Comunale viene approvato e aggiornato con cadenza annuale il Registro unico delle attività di trattamento dei dati personali, sul quale sono annotate le seguenti informazioni:
   a) il nome ed i dati di contatto del Titolare o Responsabile del trattamento e del DPO;
   b) la descrizione dei trattamenti;
   c) le finalità del trattamento;
   d) le basi giuridiche sulle quali il trattamento si fonda;
   e) le categorie di trattamenti effettuati: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
   f) le categorie di interessati;

g) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
h) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
i) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
j) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate;
k) la valutazione del rischio

2. Il Registro è tenuto dal Titolare in forma elettronica; nello stesso possono essere inserite ulteriori informazioni sul trattamento.

Articolo 29 – Valutazione di impatto sulla protezione dei dati (DPIA) (Rif. artt. 35-36 GDPR)

1. Nel caso in cui una tipologia 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 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
   La valutazione dell'impatto del medesimo trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. 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, paragrafi 4-6, del GDPR.

3. Fermo restando quanto indicato dall'art. 35, paragrafo 3, del GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) trattamenti valutativi o di attribuzione di punteggi, 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 particolari categorie di dati, di cui all'art. 9 del GDPR;
   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, sentito il DPO e l'Amministratore del sistema informatico, 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.

4. Il Titolare del trattamento garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA al Responsabile della protezione dei dati ovvero ad altro soggetto, interno o esterno al Comune. Il Titolare deve consultarsi con il DPO 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 DPO, se gli viene affidato tale incombenza da parte del Titolare del trattamento, provvede allo svolgimento della DPIA ovvero, se non gli compete la predetta incombenza, monitora lo svolgimento della DPIA. I Designati del Trattamento collaborano e assistono il Titolare del trattamento e il DPO nella conduzione della DPIA, fornendo ogni informazione necessaria. L'Amministratore del sistema informatico fornisce il necessario supporto al Titolare per lo svolgimento della DPIA.

5. Il DPO 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. L'Amministratore del sistema informatico può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. 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, paragrafo 1, del GDPR;
   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 25 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.

7. Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o dal DPO 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;
      - della 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 GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

9. Il Titolare del trattamento 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 30 – Violazione dei dati personali (Rif. artt. 33-34 GDPR)

1. Per violazione dei dati personali (in seguito "*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 Designato del trattamento è obbligato ad informare il Titolare e il DPO, 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 GDPR, sono i seguenti:
   - danni fisici, materiali o immateriali alle persone fisiche;
   - perdita del controllo dei dati personali;
   - limitazione dei diritti, discriminazione;
   - furto o usurpazione d'identità;
   - perdite finanziarie, danno economico o sociale;
   - decifratura non autorizzata della pseudonimizzazione;
   - pregiudizio alla reputazione;
   - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

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 del GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al su citato art. 33.

6. Il Titolare del trattamento 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 GDPR.

7. Il Comune di Volpiano con deliberazione di Giunta Comunale ha approvato una specifica "procedura *Data Breach*" da seguire nei casi in cui si verifichi una violazione di dati personali.

8. In appendice al presente Regolamento si allega il modello di Registro delle Violazioni, composto da una prima parte che riporta l'Indice delle Registrazioni e da una seconda parte con la scheda di dettaglio per ogni Registrazione.

Articolo 31 – Segnalazioni e richiesta di provvedimenti in autotutela

1. Qualunque soggetto, portatore di interessi pubblici o privati, a cui possa derivare un pregiudizio dal sistema di videosorveglianza, nell'ambito dei diritti di riservatezza, ha facoltà di proporre istanze o chiedere provvedimenti in autotutela da parte del titolare del trattamento dei dati personali.
2. L'istanza, la segnalazione, l'esposto o qualsiasi atto del medesimo tenore va inviato obbligatoriamente sia al RPD che al titolare del trattamento.
3. Ogni provvedimento adottato a seguito di detti atti d'impulso, compresa l'immediata archiviazione andrà gestito secondo i principi della legge 241/1990.

Articolo 32 – Tutela amministrativa e giurisdizionale

1. Qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, l'interessato può proporre reclamo al Garante della privacy italiano o ricorso dinanzi all'autorità giudiziaria.
2. Il reclamo al Garante, a mente dell'art. 140 bis del codice della privacy, non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria.
3. Il ricorso giurisdizionale, a mente dell'art. 152 del Codice della privacy, è di competenza esclusiva del giudice ordinario

Articolo 33 – Rinvio dinamico e abrogazioni

1. Per quanto non previsto in questo regolamento si dovrà fare riferimento alle norme di dettaglio o ai principi generali delle norme richiamate in premessa o agli atti di indirizzo del Garante della privacy o delle istituzioni comunitarie a ciò preposte.
2. Se il rinvio a queste norme e a questi atti di indirizzo non dovesse permettere la risoluzione o gestione della fattispecie concreta qui non regolamentata andrà posto un sintetico quesito al DPO che tempestivamente dovrà fornire una risposta o creare un'apposita interlocuzione con il Garante della privacy, nei confronti del quale è "punto di contatto" per questa amministrazione.

Articolo 34 – Entrata in vigore, pubblicazione e divulgazione del Regolamento

1. Il presente Regolamento entra in vigore il giorno stesso dell'esecutività ai sensi di legge della relativa deliberazione consiliare di approvazione.

2. Per rendere noto ai cittadini l'adozione del presente regolamento, la relativa deliberazione di approvazione sarà ripubblicata all'Albo Pretorio per ulteriori 15 giorni successivi alla prima pubblicazione.

3. Il presente Regolamento inoltre, a cura del Responsabile della Trasparenza, sarà pubblicato in modo permanente sul sito istituzionale del Comune di Volpiano, Sezione "Amministrazione trasparente", sottosezioni "Disposizioni generali", "Atti generali", "Regolamenti".

4. Il presente regolamento è trasmesso, per opportuna conoscenza, ai componenti degli organi di governo e degli organi di controllo interni, al Segretario Generale, ai Designati del Trattamento, i quali ultimi ne forniscono copia a tutte le persone autorizzate al trattamento.

Allegato A – Registro delle Violazioni

Il Registro è formato da un Indice delle Registrazioni e da una Scheda di dettaglio per ogni Registrazione. Compilare una riga dell'Indice per ogni Scheda. Allegare alle Schede copia delle eventuali Notifiche e Comunicazioni.

INDICE DELLE REGISTRAZIONI

N.	Data	Descrizione breve dell'evento	Codice Notifica	Comunicazione (Si/No)
1				
2				
3				

SCHEDA N. 1	
VERIFICA DELLA VIOLAZIONE	
Data e ora	Data e ora termine analisi della Segnalazione, da cui partono le 72 ore
Descrizione	Sintesi della Segnalazione: chi ha segnalato cosa, quando e come
Avvenuta Violazione?	No | Si
Data della violazione	Data presunta della violazione
Descrizione violazione	Descrizione sintetica dei fatti
Tipo violazione	Riservatezza, Integrità, Disponibilità
Dati personali violati	Es. dati identificativi, sanitari, giudiziari …
Interessati coinvolti	Es. cittadini, utenti di un servizio, minori, fornitori, dipendenti…
Quantità Interessati	Stima del numero di Interessati coinvolti
Sistemi Informativi	Es. Anagrafe, Contabilità, Protocollo, cartelle condivise, posta elettronica
Archivi cartacei	Es. Archivio Edilizia Privata, Fascicoli del Personale
Sedi e unità coinvolte	Es. sede principale, magazzino; Ufficio Tributi
Analisi di	Nome e ruolo di chi ha la responsabilità dell'analisi
VALUTAZIONE DEL RISCHIO	
Livello rischio	Improbabile | Probabile | Elevato
Motivazione	Sintesi delle motivazioni che portano al livello di rischio
Misure di riduzione	Misure di riduzione del rischio attuate nell'immediato
Misure successive	Misure di riduzione del rischio successivamente adottate o pianificate
Valutazione di	Nome e ruolo di chi ha la responsabilità della valutazione
NOTIFICA AL GARANTE (solo se Rischio = probabile o elevato)	
Data e ora Notifica	Data ed ora invio Notifica
Firmata da	Nome e ruolo di chi l'ha firmata
Codice Garante	Codice identificativo rilasciato dal Garante
Notifica di chiusura	Data e ora di invio Notifica di chiusura
COMUNICAZIONE AGLI INTERESSATI (solo se Rischio = elevato)	
Data avvio	Data di avvio delle comunicazioni agli interessati
Modalità	Es. lettera al domicilio, mail, avviso sul sito istituzionale