COMUNE DI PERUGIA

S.O. Contratti e Semplificazione – Vice Segretario
U.O. Risorse Umane

Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

APPROVATO CON DELIBERA DEL C.C. n. 49 dell'1.4.2019

SI ATTESTA CHE IL PRESENTE REGOLAMENTO È CONFORME AL REGOLAMENTO CARTACEO DEPOSITATO PRESSO LA SEGRETERIA DEL CONSIGLIO COMUNALE.

Sommario

Termini e definizioni

Ai fini della proposta di Regolamento comunale, si intende per:

Titolare del trattamento: il Comune che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali;

Responsabile del trattamento: il soggetto terzo, pubblico o privato (ente, azienda, professionista), che tratta dati personali per conto del Titolare del trattamento;

Sub-Responsabile del trattamento: il soggetto terzo, pubblico o privato (ente, azienda, professionista), cui un responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;

Responsabile per la protezione dati – RPD (anche noto comunemente come DPO) il soggetto incaricato dal Titolare del trattamento del ruolo di cui agli artt. 37-39 del Reg. UE 679/2016 (GDPR);

Referente interno per la protezione dei dati personali (più brevemente "**referente privacy**"), la persona fisica che il titolare del trattamento ha individuato e designato, ai sensi dell'articolo 2-quaterdecies Dlgs 196/03, sotto la propria responsabilità ed autorità e nell'ambito del proprio assetto organizzativo, ed a cui ha attribuito specifici compiti e funzioni connessi al trattamento di dati personali [eventualmente con delega di funzioni];

Soggetto designato, la persona fisica che il titolare del trattamento ha individuato, ai sensi dell'articolo 2-quaterdecies Dlgs 196/03, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, ed ha cui ha attribuito specifici compiti e funzioni connessi al trattamento di dati personali [eventualmente con delega di funzioni];

Soggetto autorizzato al trattamento, la persona fisica in possesso di apposita formazione ed istruzione, che si sia impegnata alla riservatezza od abbia un adeguato obbligo legale di riservatezza autorizzata ad accedere ai dati personali (in precedenza "incaricato").

Registro delle attività di trattamento, l'elenco dei trattamenti in forma cartacea o elettronica tenuti dal Titolare del trattamento,

DPIA - Data Protection Impact Assessment - "**Valutazione d'impatto sulla protezione dei dati"**, una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

Regolamento europeo (detto anche GDPR o RGPD) il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 sulla protezione dei dati.

Violazione dei dati personali (in seguito anche "*data breach*"), una violazione di sicurezza che comporta, accidentalmente o in modo intenzionale, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati.

Art.1 - Oggetto

1. Il presente Regolamento stabilisce modalità e procedure relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Scopo del presente regolamento è quello di proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. Il presente regolamento stabilisce ed indica le misure tecniche e organizzative adeguate da mettere in atto per garantire un livello di sicurezza adeguato al rischio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo e del DLGS 196/03 relativi alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Perugia.

Art. 2 - Titolare del trattamento

1. Il Comune di Perugia, rappresentato ai fini previsti dal RGPD dal Sindaco *pro tempore*, è il Titolare del trattamento dei dati personali.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali e garantisce che i dati saranno:
   a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
   b. 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 sarà, conformemente all'articolo 89, paragrafo 1 del Regolamento europeo, 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, conformemente all'articolo 89, paragrafo 1 del Regolamento europeo, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento 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 accidentali («integrità e riservatezza»).
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate, tra cui il presente Regolamento comunale, per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
4. Le misure adeguate 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 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. 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.
5. Il Titolare adotta misure appropriate per fornire all'interessato:
   a. le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
   b. le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

6. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art.11.
7. Il Titolare, inoltre, provvede a:

a. nominare il Referente interno per la protezione dei dati personali, specificandone compiti e funzioni, secondo le previsioni dello Schema generale di organizzazione vigente;
b. nominare i dirigenti incaricati quali Designati per la protezione dei dati personali in relazione alle funzioni e ai compiti a questi assegnati in base allo Schema generale di organizzazione. Procede altresì a specificare compiti e funzioni di ogni soggetto designato in materia di protezione dei dati personali;
c. nominare il Responsabile della Protezione dei Dati;
d. stipulare, direttamente o per il tramite dei soggetti designati, un'apposita clausola - in caso di affidamento all'esterno di servizi o attività comportanti il trattamento di dati da parte di soggetti terzi - per attribuire la qualità di Responsabile del trattamento, ai sensi dell'art. 28 del Regolamento europeo – GDPR 2016/679, alla persona fisica o giuridica affidataria;
e. individuare e nominare gli Amministratori di Sistema.

8. 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, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la co-titolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, 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 RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
9. Il Comune favorisce, ove possibile, 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 RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.
10. In presenza di convenzioni di accesso con enti ed organismi statali o regionali, allorché si tratti di titolari che determinano autonomamente le finalità ed i mezzi del trattamento, il titolare procederà alla cessione dei dati in forza di specifica disposizione di legge, di regolamento o di accordo, avendo cura di specificare limiti e finalità del trattamento.

Art. 3 - Finalità del trattamento

1. I trattamenti sono compiuti dal Comune per le finalità individuate e specificate dettagliatamente nel Registro dei Trattamenti.
2. A mero titolo di esempio, tali finalità possono riguardare:

a. l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (la finalità del trattamento è stabilita dalla fonte normativa che lo disciplina);
b. l'adempimento di un obbligo legale al quale è soggetto il Comune (la finalità del trattamento è stabilita dalla fonte normativa che lo disciplina);
c. l'esecuzione di un contratto con soggetti interessati.

3. Nel trattare i dati ai sensi del precedente comma 2, il Comune non è tenuto a richiedere il consenso dell'interessato.
4. Il Comune potrà altresì trattare i dati per ulteriori e specifiche finalità, diverse da quelle previste dalla legge, purché l'interessato esprima il proprio consenso al trattamento.
5. Nel rispetto delle prescrizioni del Regolamento UE, l'Amministrazione comunale favorisce la trasmissione di dati o documenti fra le banche dati e gli archivi del Comune, degli Enti Territoriali, degli Enti pubblici, dei gestori od esercenti di pubblici servizi, degli incaricati di pubblico servizio, operanti nell'ambito dell'Unione Europea. Nella trasmissione deve essere indicato il nominativo del titolare e del responsabile del

trattamento, le finalità e le operazioni del trattamento, le modalità di connessione, di trasferimento e di comunicazione dei dati, nonché le misure di sicurezza.

Art. 4 - Circolazione dei dati all'interno del Comune

1. La comunicazione dei dati all'interno della struttura organizzativa del Comune, per ragioni d'ufficio, non è soggetta a limitazioni particolari, salvo quelle espressamente previste da leggi e regolamenti. Non si considera comunicazione di dati a terzi la trasmissione e l'accesso di dati da parte del personale dipendente del Comune, qualora il trasferimento e l'accesso avvenga per ragioni di ufficio, nell'esercizio delle mansioni proprie di ciascun dipendente e per lo svolgimento delle funzioni istituzionali.
2. Il Designato del trattamento dei dati, specie se la comunicazione concerne dati particolari, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone, limitando l'accesso o la trasmissione dei dati sensibili e giudiziari ai soli casi di effettiva necessità per lo svolgimento delle funzioni ed attività comunali.

Art. 5 - Soggetti designati

1.Il Titolare individua uno o più soggetti designati del trattamento 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 art.8 – Sicurezza del trattamento, rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.
2. I soggetti designati, identificati ai sensi della normativa italiana vigente, sono nominati mediante decreto di incarico 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, mediante rinvio allo schema generale di organizzazione vigente e al registro dei trattamenti;
c. gli obblighi ed i diritti del Titolare del trattamento;
d. le funzioni ed i poteri attribuiti al soggetto designato.

3. Il soggetto designato provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

a. ad autorizzare al trattamento dei dati tutti i dipendenti assegnati;
b. alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
c. all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
d. alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
e. alla stipulazione di un'apposita clausola - in caso di affidamento all'esterno di servizi o attività comportanti il trattamento di dati da parte di soggetti terzi - per attribuire la qualità di Responsabile del trattamento, ai sensi dell'art. 28 del Regolamento europeo – GDPR 2016/679, alla persona fisica o giuridica affidataria;
f. ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
g. ad 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 che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art. 6 - Responsabili del trattamento

1. Il Titolare può avvalersi, per il trattamento di dati, di soggetti pubblici o privati che, in qualità di Responsabili del trattamento ai sensi dell'articolo 28 GDPR, forniscano le garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

2. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che individui la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a. tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b. garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c. adotti tutte le misure richieste ai sensi dell'articolo 32 GDPR;
d. non ricorra ad un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche. Se un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile;
e. assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
f. su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
g. metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato.

3. Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

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

5. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

6. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento.

Art. 7 - Responsabile della protezione dati

1. Il Responsabile della protezione dei dati può essere un dipendente del titolare oppure assolvere i suoi compiti in base ad un contratto di servizi.

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. 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 di interessi. L'assenza di conflitti di interessi 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:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- 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;
- 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;
- 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:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Responsabile del trattamento;
- 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:

- 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;
- tempo sufficiente per l'espletamento dei compiti affidati al RPD;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, oppure tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale);
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

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. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - o al Responsabile del trattamento.

9. 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.

Art. 8 - Sicurezza del trattamento

1. Il Comune di Perugia e ciascun Responsabile del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

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

2. Nel valutare l'adeguatezza del livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. Viene ritenuta misura di sicurezza essenziale la formazione e l'istruzione di chiunque agisca sotto l'autorità del Titolare ed abbia accesso a dati personali.

4. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di 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.

5. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.
6. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

Art. 9 - Registro delle attività di trattamento

1. Il Titolare, direttamente o tramite il proprio Referente per la protezione dei dati personali, tiene aggiornato il Registro delle attività di trattamento come previsto dall'articolo 30 GDPR.
2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, 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.

Art. 10 - Registro delle categorie di attività trattate dal Responsabile

1. Il Registro delle categorie di attività trattate da ciascun Responsabile di cui al precedente art. 6, reca le seguenti informazioni:
   - il nome ed i dati di contatto del Responsabile del trattamento e del RPD;
   - le categorie di trattamenti effettuati da ciascun Responsabile: 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;
   - l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   - il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea.

Art. 11 - Valutazioni d'impatto sulla protezione dei dati

1. 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. La 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, pp. 4-6, RGDP.
3. La DPIA è sempre effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche.
4. 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.
5. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, 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. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

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 da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.
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 deve essere specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
10. Se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato il Titolare deve consultare il Garante Privacy prima di procedere al trattamento. Il Titolare consulta il Garante Privacy anche nei casi in cui vi sia 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.

Art. 12 - Violazione dei dati personali

1. In presenza di una violazione dei dati personali, il Titolare provvede alla notifica della violazione al Garante Privacy, a meno che sia improbabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.
2. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, procede senza ingiustificato ritardo ad informare questi ultimi, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi, i possibili rischi ed eventuali contromisure.
3. 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.
4. 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.

5. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, non appena viene a conoscenza della violazione.

Art. 13 - Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.