

COMUNE DI CARPINETO ROMANO
(Città Metropolitana di Roma Capitale)

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 di Consiglio Comunale n. 14 del 23.05.2018

INDICE:

Art. 1 - Oggetto

Art. 2 - Titolare del trattamento

Art. 3 - Finalità del trattamento

Art. 4 - Persone Autorizzate al Trattamento - Incaricati

Art. 5- Responsabili del Trattamento

Art. 6 - Responsabile della protezione dati

Art. 7 - Sicurezza del trattamento

Art. 8 - Registro delle attività di trattamento

Art. 9 - Registro delle categorie di attività trattate

Art. 10 - Valutazione d'impatto sulla protezione dei dati

Art. 11 - Violazione dei dati personali

Art. 12 - Rinvio

Art. 1

Oggetto

Il presente Regolamento ha per oggetto misure procedurali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione dell'allegato Regolamento Europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Carpineto Romano.

Art.2

Titolare del trattamento

1. Il Comune di Carpineto Romano, ai fini previsti dal RGPD è il Titolare del trattamento dei dati personali contenuti in archivio, o destinati a figurarvi, interamente o parzialmente automatizzato (di seguito indicato con "Titolare).
2. Il Sindaco pro tempore è il rappresentante del Titolare
3. Il Titolare è competente per il rispetto dei principi applicabili al trattamento dei dati personali di cui all'art. 5 RGDP, ossia i principi di liceità, correttezza e trasparenza.
4. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Tali misure sono riesaminate e aggiornate se necessario.

A tale scopo il Titolare :

- può delegare le relative funzioni a Dirigente/Responsabile Posizione Organizzativa in possesso di adeguate competenze e designato da apposito atto formale, fermo restando la sua responsabilità nel trattamento dei dati personali ai sensi dell'art. 24 del RGPD.;
 - adotta le misure tecniche e organizzative, quali la pseudonimizzazione e la minimizzazione, fin dalla fase di progettazione(privacy by design) per garantire che siano trattati per impostazione predefinita (privacy by default)solo i dati necessari per ogni specifica finalità di trattamento;
 - fornisce all'interessato in forma concisa , trasparente ,intelligibile e facilmente accessibile con un linguaggio semplice e chiaro:
- A. tutte le informazioni di cui all' art. 13 del RGPD qualora i dati personali siano raccolti presso lo stesso interessato;

- B. tutte le informazioni di cui all' art. 14 del RGPD qualora i dati personali non siano raccolti presso lo stesso interessato;
- C. tutte le informazioni per agevolare l'esercizio dei diritti ai sensi degli articoli da 15 a 22 GDPR;
- D. ogni comunicazione relativa ad eventuali violazione dei dati personali (data breach) ai sensi dell'art. 34 del RGPD.

Gli interventi necessari per l'attuazione delle misure sono decise dal titolare e 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.

4. 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. 9.

5. Il Titolare, nella persona del rappresentante del Titolare, ossia il Sindaco p.t. inoltre, provvede a:

- A. designare, con atto formale di nomina, quali Responsabili del trattamento interni, le figure apicali dei Dirigenti/Responsabili P.O. e dei Funzionari 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. designare con atto formale di nomina, quali Responsabili del trattamento esterno, i soggetti pubblici o privati i quali, per conto del titolare del trattamento, in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, trattano i dati personali degli interessati, raccolti in banche dati gestite esternamente al Comune per la realizzazione di attività connesse alle attività istituzionali;
- C. predisporre l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente (in relazione alle dimensioni organizzative del Comune) dei quali il Titolare può avvalersi, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

D. designare con atto formale di nomina il Responsabile per la Protezione dei dati interno od esterno all'ente;

6. Contitolarità: Qualora due o più titolari del trattamento, determinano congiuntamente, mediante accordo interno, le finalità ed i mezzi del trattamento, si realizza la contitolarità del trattamento di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi derivanti dal RGPD, 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 (informativa), fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

7. Il Titolare favorisce 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.

Art.3

Finalità del trattamento

1. Il Titolare raccoglie i dati personali per finalità determinate, esplicite e legittime. I trattamenti dei dati personali operati dal titolare sono compiuti per le seguenti finalità:

- A. l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Rientrano in questo ambito i trattamenti compiuti per:
- l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
 - la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
 - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione. 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;
- D. il perseguimento del legittimo interesse del titolare;
- E. per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art.4

Persone autorizzate al trattamento - Incaricati (art. 4, n. 10, del RGPD)

Incaricato del Trattamento interno al Comune

Un Dirigente/Responsabile P.O. o più Dirigenti/Responsabili P.O. delle strutture di massima dimensione in cui si articola l'organizzazione dell'Ente, è nominato "Incaricato del Trattamento di dati personali" di tutte le banche dati presenti e site all'interno del Comune nell'articolazione organizzativa di rispettiva competenza. L'incaricato del trattamento deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, individuato per iscritto e che opera sotto la diretta autorità del titolare, attuandone le istruzioni.

Possono essere designati quali Incaricati del Trattamento solo ed esclusivamente le persone fisiche e non anche le entità personificate.

Gli Incaricati, sono designati, di norma, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;

L'incarico del trattamento di dati personali connesso all'espletamento dei compiti istituzionali dell'amministrazione, deve svolgersi sotto la diretta sorveglianza e secondo le istruzioni di questa, che conserva la qualità di "titolare del trattamento", non deve comportare decisioni di fondo sulle finalità e sulle modalità di utilizzazione dei dati, ma limitati margini di autonomia in ordine al concreto svolgimento del servizio ed a scelte tecnico-operative dettagliatamente specificato nell'atto formale di incarico.

Il Titolare può nominare sub - incaricati, i quali sono anche essi sotto la sua diretta responsabilità, con atti formali scritti.

In assenza di una formale designazione come incaricati del trattamento, i dipendenti delle pubbliche amministrazioni che, per lo svolgimento dei propri compiti, vengono a conoscenza di dati personali, devono essere considerati come soggetti terzi rispetto alle amministrazioni stesse, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento.

Tale designazione è, infatti, indispensabile, in quanto permette di considerare legittimo il flusso delle informazioni personali nell'ambito degli uffici e tra i dipendenti dell'amministrazione titolare del trattamento

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun incaricato designato.

Le Persona incaricata del trattamento con apposito atto formale in forma scritta deve essere in possesso di apposita formazione ed istruzione ed è sottoposto ad obbligo legale di riservatezza

Art.5

Responsabile del Trattamento

Sono nominati Responsabili del Trattamento:

3. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento esterni, forniscano le garanzie di cui al comma 1, stipulando un **contratto** in forma scritta (o altro atto giuridico conforme al diritto nazionale) che specifichino la materia disciplinata, la natura e la finalità perseguita, la tipologia dei dati, la categoria degli interessati, la durata del trattamento, gli obblighi e i diritti del titolare del trattamento e le modalità di trattamento.
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. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile 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.

6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia nominato Persona autorizzata al trattamento con apposito atto formale in forma scritta e sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
7. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla RGPD e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
 - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare e a cooperare con l'autorità di controllo mettendo a disposizione tali registri per monitorare detti trattamenti;
 - all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti di cui all'art. 32 RGPD;
 - alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
 - 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;
 - 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.
 - devono individuare con atto formale al loro interno gli incaricati e i sub incaricati quali persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del Responsabile del Trattamento

Art.6

Responsabile della protezione dati

1) Obbligo di designazione:

La designazione di un RPD è obbligatoria ogniqualvolta il trattamento dei dati personali è effettuato da una autorità pubblica o da un organismo pubblico.

Il Comune di Carpineto Romano è obbligato a designare il Responsabile per la Protezione dei Dati (diseguito RPD) mediante procedura prevista da norma di legge, nelle seguenti modalità:

a) RPD interno

Il RPD può essere scelto fra i dipendenti del Comune di qualifica non inferiore alla cat. D (oppure C negli enti di minore dimensione), purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il Titolare ed il Responsabile del trattamento provvedono affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

b) RPD esterno

Il RPD, persona fisica, in caso di mancata individuazione di figura interna al comune, è selezionato mediante procedura prevista a norma di legge, fra soggetti aventi le medesime qualità professionali richieste al dipendente, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili; i compiti attribuiti al RPD sono indicati in apposito contratto di servizi. Il RPD è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare ed al Responsabile del trattamento. Nel caso di Comuni di minori dimensioni demografiche, è possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più Comuni mediante esercizio associato della funzione nelle forme previste dal D.Lgs. 18 agosto 2000 n. 267.

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 personali, 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;

e.——sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d.——fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi al RGPD;

e.——cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante della protezione dei dati;

f.——supervisiona circa la regolare tenuta dei registri di cui ai successivi artt. 7 e 8;

g.——Il RPD può svolgere altri compiti e funzioni . Il Titolare o il Responsabile del Trattamento devono assicurarsi che tali ulteriori compiti e funzioni non diano adito a conflitto di interessi strettamente connessa agli obblighi di indipendenza del RPD.

2. 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 dal titolare determini condotte difformi da quelle raccomandate dal RPD, è necessario che il titolare motivi specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. 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:

- procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- 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.

4. 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.

5. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili (in relazione alle dimensioni organizzative del Comune):

- Il Titolare del trattamento
- 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.

6. 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, ovvero (in relazione alle dimensioni organizzative dell'Ente) tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale);
- 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.

7. 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 Rappresentante del Titolare - (Sindaco p.t. o suo delegato) - od al Responsabile del trattamento. 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.7

Sicurezza del trattamento

1. Il Titolare Comune di Carpineto Romano e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato 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 resilienza dei sistemi e dei servizi che trattano 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 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.

4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali può essere dimostrata attraverso l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. Il Comune di Carpineto Romano e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque sia stato incaricato, con atto formale, ad effettuare accessi in banche dati e trattamenti di dati per conto del titolare o/o responsabile del trattamento..

6. 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.

7. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.Lgs. n. 193/2006).

Art.8

Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

- il nome ed i dati di contatto del Comune, del Sindaco e/o del suo Delegato ai sensi del precedente art.2, eventualmente del Contitolare del trattamento, del RPD;
- le finalità del trattamento;
- la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

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, secondo lo schema allegato A al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.

3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

4. Il Titolare può decidere di tenere un Registro unico dei trattamenti che contiene le informazioni di cui ai commi precedenti e quelle di cui al successivo art. 8, sostituendo entrambe le tipologie di registro dagli stessi disciplinati, secondo lo schema allegato C al presente Regolamento. In tal caso, il Titolare delega la sua tenuta al Responsabile unico del trattamento di cui al precedente art. 4 o, comunque, ad un solo Responsabile del trattamento, ovvero può decidere di affidare tale compito al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Art.9

Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Responsabile di cui al precedente art. 4, reca le seguenti informazioni:

- a. il nome ed i dati di contatto del Responsabile del trattamento e del RPD;
- b. 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;
- c. l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- d. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema allegato B al presente regolamento.

3. Il Responsabile del trattamento può decidere di affidare al RPD, il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile del Trattamento.

Art.10

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 del trattamento di cui trattasi alle norme del RGPD.

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 ove redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

- a. trattamenti di valutazione sistematica, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
- b. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
- c. monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
- d. trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
- e. trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

- f. combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
- g. dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
- h. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
- i. tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

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

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. 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.

5. 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.

6. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;

- 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;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente.

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.

7. 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.

8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

9. 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.

10. 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.

(eventuale) 11. E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art. 11

Violazione dei dati personali

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 Responsabile del trattamento è obbligato ad informare il Titolare, e il RPD, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- 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 RGPD, ed anche la comunicazione all’interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art.12

Rinvio

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

GLOSSARIO REGOLAMENTO

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

◊ Titolare del trattamento

l'autorità pubblica (Sindaco p.t.) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.

◊ Responsabile del trattamento:

il Dirigente/Responsabile P.O., oppure il soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.

◊ Sub-Responsabile del trattamento: il dipendente della struttura organizzativa del Comune, incaricato dal Responsabile del trattamento con atto formale, per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento (elabora o utilizza materialmente i dati personali).

◊ Responsabile per la protezione dati – RPD il dipendente della struttura organizzativa del Comune, il professionista privato o persona fisica di impresa esterna, incaricati dal Titolare o dal Responsabile del trattamento.

◊ Registri delle attività di trattamento elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento secondo le rispettive competenze.

◊ DPIA - Data Protection Impact Assessment” - “Valutazione d’impatto sulla protezione dei dati è 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.

◊ Garante Privacy il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente.

GLOSSARIO REGISTRI

Ai fini delle proposte dei registri, si intende per:

◊ Categorie di trattamento

Raccolta; registrazione; organizzazione; strutturazione; conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto od interconnessione; limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.

◊ Categorie di dati personali

Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale. Dati inerenti lo stile di vita Situazione economica, finanziaria, patrimoniale, fiscale.

Dati di connessione: indirizzo IP, login, altro.

Dati di localizzazione: ubicazione, GPS, GSM, altro.

Dati sensibili : origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici intesi ad indentificare in modo univoco una persona fisica, dati relativi alla salute, relativi alla vita sessuale o all'orientamento sessuale della persona, relativi a condanne penali.

◊ Finalità del trattamento

Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico; la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica; l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune. Adempimento di un obbligo legale al quale è soggetto il Comune. Esecuzione di un contratto con i soggetti interessati. Altre specifiche e diverse finalità.

◊ Misure tecniche ed organizzative

Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che 36 trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi.

Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) - adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.

Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico - adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.

Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

◊ Categorie interessati

Cittadini residenti; minori di anni 16; elettori; contribuenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; altro.

◊ Categorie destinatari

Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.