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 Deliberazione del Consiglio Comunale n. 6 del 30/04/2018

Sommario

Art. 1

Oggetto

1 Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento Europeo (General Data Protection Regulation del 27 aprile 2016, n. 679, di seguito indicato con "RGDP", 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 Ussassai.

Art. 2

Finalità del trattamento

1 I trattamenti sono compiuti dal Comune per le seguenti finalità:

a. L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:

i. 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;

ii. La gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;

iii. L'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione. La finalità del trattamento è stabilità dalla fonte normativa che lo disciplina;

b. L'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilità dalla fonte normativa che lo disciplina;

c. L'esecuzione di un contratto con soggetti interessati;

d. Per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 3

Titolare del Trattamento

1 Il Comune di Ussassai, rappresentato ai fini previsti dal RGPD dal Sindaco Pro Tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco può delegare le relative funzioni a Dirigente/Responsabile di Posizione Organizzativa (P.O.), in possesso di adeguate competenze.

2 Il Titolare p responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'articolo 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3 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.

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 del 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.

4 Il Titolare adotta misure appropriate per fornire all'interessato:

a. Le informazioni indicate dall'articolo 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b. Le informazioni indicate dall'articolo 14 RGPD, qualora i dati personali non siano disponibili presso lo stesso interessato.

5 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", secondo uno dei due modelli allegati al presente regolamento di cui ai numeri: "01 – dpia –" e/o n. "02 - dpia - alternativo") ai sensi dell'articolo 35, RGPD, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 9 del presente regolamento.

6 Il Titolare, inoltre, provvede a:

a. Designare i responsabili del trattamento nelle persone dei Responsabili di Posizione Organizzativa 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, rispettando le prescrizioni di cui all'articolo 28, paragrafo 3 del RGPD. Per il trattamento di dati il Titolare può anche avvalersi di soggetti pubblici o privati, ed anche in tale ultimo caso dovranno essere rispettate le prescrizioni di cui all'articolo 28, paragrafo 3 del RGPD;

b. Nominare il Responsabile della protezione dei dati;

c. Nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

d. Predisporre l'eventuale elenco dei Responsabili del trattamento dei servizi in cui si articola l'organizzazione dell'Ente, pubblicandolo nella sezione amministrazione trasparente-organizzazione-articolazione degli uffici, ed aggiornandolo ad ogni mutamento di nomina.

7 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 contitolarità di cui all'articolo 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di tutela dei dati personali, con particolare rifermento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto id contatto comune per gli interessati.

8 Il Comune 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 contribuite alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei responsabili del trattamento.

Art. 4
Responsabile del Trattamento

1 Un Responsabile di Posizione Organizzativa o più Responsabili di Posizione Organizzativa è nominato unico Responsabile del Trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile Unico deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto tutte le misure tecniche ed organizzative di cui all'articolo 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.

2 I Dipendenti del Comune, Responsabili del trattamento, sono designati, di norma, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

- La materia tratta, 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;
- Gli obblighi ed i diritti del Titolare del Trattamento.

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

3 Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.

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

5 È 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; tale nomina può essere fatta previa autorizzazione scritta, specifica o generale del Titolare del Trattamento ai sensi dell'articolo 28, paragrafo 2 del RGPD. 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 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 legge 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;
- All'adozione di idonee misure tecniche ed organizzative adeguate per garantire la sicurezza dei trattamenti;

- Alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- Se demandato dal Titolare alla designazione del Responsabile per la Protezione dei Dati (RPD o DPO: Data Protection Officer);
- 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.

Art. 5
Responsabile per la protezione dati

1 Il Responsabile per la protezione dei dati (in seguito indicato con "RDP", detto anche DPO: Data Protection Officer) è individuato nella figura unica di un dipendente del Comune, avente un inquadramento professionale non inferiore alla categoria D, 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. L'individuazione può essere disposta anche nei confronti di un soggetto, anche esterno all'organizzazione comunale, da parte di più Comuni mediante esercizio associato della funzione nelle forme previste dal D. Lgs. 18 agosto 2000, n. 267. Nel caso di assenza di figure professionali idonee è possibile procedere alla individuazione della figura rivolgendosi ad un professionista scelto tramite procedura ad evidenza pubblica.
Il RDP è incaricato, anche ai sensi dell'articolo 39 del RGPD, dei seguenti compiti:
- 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 n relazione al rischio riscontrato;
- Sorvegliare l'osservanza del RGPD e della 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;
- Sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;
- 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:
  i. Se condurre o meno una DPIA;
  ii. Quale metodologia adottare nel condure una DPIA;
  iii. 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;

iv. Se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno al trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

- 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'articolo 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;
- La tenuta dei registri di cui ai successivi articoli 7 e 8;
- 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, ai sensi dell'articolo 38 del RGPD.

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 Responsabili di Posizione Organizzativa 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 o 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.

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 stessi incompatibili:

- Il Responsabile per la prevenzione della corruzione e per la trasparenza;
- Il Responsabile del Trattamento;
- Qualunque incarica 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 Responsabili di Posizione Organizzativa 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;
- 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;
- Acceso 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 istruizoni in merito al loro svolgimento né sull'interpretazione da dare ad 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 – 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. 6
Addetto al trattamento

1 L'Addetto al trattamento è colui che materialmente tratta i dati personali.

2 Il Titolare e il Responsabile del trattamento si assicurano che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito, salvo che il loro trattamento sia richiesto dal diritto dell'Unione Europea o degli Stati membri

3 L'addetto al trattamento è persona fisica, interna o esterna all'Ente, caratterizzata da appropriate attribuzioni di responsabilità e sia stato sensibilizzato e formato in modo appropriato. Per la formazione deve intendersi un programma di approfondimento relativo, almeno, alle seguenti conoscenze:

a. Breve panoramica dell'evoluzione legislativa in materia di protezione dei dati personali;
b. Obblighi generali nel trattamento di dati personali;
c. Cautele particolari per i dati particolarmente sensibili;
d. I profili professionali coinvolti, illustrando in particolare, con nome e cognome, i soggetti cui l'addetto deve fare riferimento nella sua quotidiana attività;
e. I rapporti con l'interessato al trattamento: cosa dire e cosa non dire, sia di personale, sia in comunicazioni telefoniche;
f. Le modalità di custodia e controllo degli stessi dati, accessibili mediante sistemi informativi: suggerimenti sulla scelta e la custodia sicura delle parole chiave;
g. Le modalità di cancellazione di dati personali obsoleti, come comportarsi davanti alla fotocopiatrice;
h. Responsabilità civile e penale e sanzioni;
i. A chi rivolgersi per ottenere delucidazioni in caso di dubbio.

4 L'Addetto al trattamento deve, tra le altre, rispettare e garantire la riservatezza dei dati trattati, specificando che tale obbligo alla riservatezza rimane in vigore anche dopo che l'addetto abbia esaurito il trattamento dei dati affidato.

Art. 7
Sicurezza del Trattamento

1 Il Comune di Ussassai 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 di 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; controllo sugli accessi, come la registrazione; porte, armadi e contenitori dotati di serrature e ignifughi, sistemi di copiatura e conservazione di archivi elettronici; gestione delle chiavi e serrature; 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 RGPD 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.

5 Il Comune di Ussassai e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6 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, e nella sezione Privacy se 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, del D. Lgs. 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:

a. Il nome ed i dati di contatto del Comune, del Sindaco e/o suo delegato ai sensi del precedente articolo 3, eventualmente del contitolare del trattamento, del RPD;
b. La finalità del trattamento;
c. La sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d. Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e. L'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

f. Ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g. Il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente articolo 7.

2 Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente articolo 3, presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea, secondo lo schema allegato "C" al presente Regolamento; nello stesso possono esser 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 articolo 9, sostituendo entrambe le tipologie di registro dagli stessi disciplinati, secondo lo schema allegato "E" al presente Regolamento. In tal caso, il titolare delega la sua tenuta al Responsabile unico del Trattamento di cui al precedente articolo 5, 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 elemnto 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 articolo 5, 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, 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 articolo 7.

2 Il Registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema allegato "D" 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.

Art. 10
Valutazione di 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'articolo 35 RGPD, 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'articolo 35, paragrafi 4-6 del RGPD.

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

a. Trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c. Monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di datti attraverso rei 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'articolo 9 del RGPD;

e. Trattamenti di dati su larga scala, tenendo conto: del 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 applicazioni 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 aa 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 necessarie 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'articolo 35, paragrafo 1 del RGPD;

b) Se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;

c) Se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;

d) Se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. 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 minimo 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 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 e 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 originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

11 Ove ritenuto opportuno è 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, 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[1] 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 e/o 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'articolo 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato articolo 33[2].

---

[1] I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazione, furto o usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se non sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

[2] *Articolo 33-* **Notifica di una violazione dei dati personali all'autorità di controllo**

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

6 Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esser relative, le conseguenze e i provvedimenti adottati o che intende adottare per provi 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

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

---

3. La notifica di cui al paragrafo 1 deve almeno:
   a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
   c) descrivere le probabili conseguenze della violazione dei dati personali;
   d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.