Comune di Forlì

SERVIZIO SEGRETERIA E AFFARI GENERALI

Regolamento comunale di attuazione del Regolamento UE 2016/679 relativo al trattamento dei dati personali

Approvato con Deliberazione Consiliare nr. 78 del 28/11/2022

INDICE

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 "**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 Forlì (FC).

Art.2 Titolare del trattamento

1. Il Comune di Forlì, 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 Segretario/Dirigenti in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 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 a 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 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'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.

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") 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. 10.

6. Il Titolare, inoltre, provvede a:
   a) Designare uno o più **Designati speciali al trattamento**, eventualmente uno per ogni singolo servizio in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;
   b) Nominare il **Responsabile della Protezione dei Dati**;
   c) Nominare quale **Responsabile esterno 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;

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'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.

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

   a) Esecuzione di un *compito di interesse pubblico o connesso all'esercizio di pubblici poteri*. Rientrano in questo ambito i trattamenti compiuti per:
      - l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
      - la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
      - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.
   b) Attuazione di *atti amministrativi generali (art. 2-ter Codice privacy novellato dalla legge 205/2021)*, che evidenzino un trattamento necessario per svolgere compiti di pubblico interesse o nell'esercizio di pubblici poteri.
   c) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
   d) l'esecuzione di un contratto con soggetti interessati;
   e) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art.4 Designato (speciale) al trattamento

1. In applicazione del ***Principio di titolarità diffusa*** secondo il quale l'intreccio tra ruolo e attività del titolare del trattamento e l'ordinamento degli Enti locali porta a non individuare il titolare nel sindaco, ma ad un modello di "titolare diffuso", esattamente come avviene più in generale per le altre funzioni degli enti, il Sindaco, in qualità di legale rappresentante dell'Ente, Titolare del trattamento ai sensi dell'art. 4, par. 1, n. 7 del GDPR, e sotto la propria responsabilità, designa al trattamento i Dirigenti preposti ai Servizi in cui si articola l'organizzazione comunale, delegando loro specifici compiti e funzioni in ordine alle finalità e ai mezzi connessi al trattamento di dati personali, funzionali ai compiti di ciascuna articolazione organizzativa. Il designato deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 7 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.
2. Il Designato al trattamento sovrintende, relativamente alle banche dati degli ambiti di competenza, a tutte le attività stabilite dalla legge ed esercita tutti i compiti e le funzioni allo stesso affidati dal Titolare,

indicati specificamente nell'atto di delega, e concorre a realizzare il modello organizzativo privacy e, in particolare:

a) rende le informazioni sul trattamento dei dati personali previste dagli artt. 13 e 14 del GDPR, prima della raccolta dei dati, agevolando l'esercizio dei diritti dell'interessato;
b) per i trattamenti che hanno come base giuridica il consenso, adotta le misure organizzative atte a garantire la conservazione della copia del consenso acquisito;
c) predispone e aggiorna i Registri di cui al successivo articolo 8;
d) mette in atto misure tecniche ed organizzative adeguate, efficaci e proporzionate allo scopo di garantire la sicurezza del trattamento ai sensi del successivo articolo 7;
e) riesamina ed aggiorna le misure di sicurezza relative alle banche dati digitali, d'intesa con il Responsabile della Transizione Digitale, con il supporto del DPO;
f) interloquisce e collabora con il DPO allo scopo di attuare prescrizioni e raccomandazioni emerse in sede di audit interni. Predispone inoltre, sempre in accordo con il DPO, un calendario di audit da svolgere congiuntamente, nei confronti dei Responsabili del trattamento e dei loro eventuali Sub-Responsabili del trattamento che trattano dati personali per conto dell'Amministrazione, compresi audit a campione ovvero a rotazione;
g) individua, contrattualizza e nomina i Responsabili esterni del trattamento;
h) relativamente alle banche dati degli ambiti di competenza, individua le modalità più opportune per autorizzare al trattamento dei dati personali e nomina le persone che operano sotto la sua diretta autorità, nel rispetto delle misure di sicurezza previste e delle istruzioni impartite. L'atto di incarico degli **autorizzati al trattamento** deve disciplinare:
    i) la materia trattata, la durata, la natura e la finalità di trattamento o dei trattamenti assegnati;
    ii) il tipo di dati personali oggetto di trattamento e le categorie di interessati;
    iii) gli obblighi e i diritti del Titolare del trattamento;
    iv) le misure di sicurezza;
    v) le istruzioni per il corretto trattamento.

3. effettua con le modalità di cui al successivo articolo 10, in accordo con il DPO, per la parte di competenza, prima di procedere al trattamento, la valutazione d'impatto sulla protezione dei dati nei casi in cui essa è obbligatoria o comunque opportuna;
4. svolge, con il supporto del DPO e con l'assistenza del Gruppo data breach, l'attività preliminare nei casi di presunto incidente di sicurezza di cui venga a conoscenza, secondo la procedura di gestione dei data breach di cui al successivo articolo 11.

Art.5 Responsabile esterno del trattamento

1. Il Dirigente designato può avvalersi di soggetti esterni che svolgono per conto dell'Ente servizi o attività che implicano il trattamento di dati personali. Detti soggetti sono scelti in virtù dei requisiti di esperienza, capacità e affidabilità, in relazione alle peculiarità della materia di che trattasi.
2. Il Dirigente individua, contrattualizza e nomina i Responsabili del trattamento ai sensi dell'art. 28 del GDPR, avendo cura di specificare, fin dalla fase di scelta del contraente, le caratteristiche professionali e organizzative che essi devono possedere, in relazione alle peculiarità del servizio o del lavoro affidato;
3. Il Responsabile del trattamento - solo se autorizzato preventivamente per iscritto dal Dirigente - può avvalersi di soggetti terzi, cosiddetti Sub-Responsabili, e comunque nel rispetto degli obblighi contrattuali che lo legano al Titolare.
4. Il Dirigente, per mitigare i rischi derivanti dal trattamento, mette in atto opportuni strumenti che gli consentono di monitorare le attività affidate in outsourcing e trasmette periodicamente le risultanze all'Ufficio del DPO.
5. Le nomine dei Responsabili del trattamento sono annotate nel Registro delle attività di trattamento, ai sensi dell'art. 30 del GDPR.

Art.6 Responsabile della Protezione Dati ("RPD" o "DPO")

1. Il Sindaco designa il Responsabile della protezione dei dati, in inglese, Data Protection Officer in un soggetto esterno scelto con procedura di evidenza pubblica. L'individuazione del RPD/DPO avviene in funzione delle qualità professionali e di esperienza, delle conoscenze specialistiche della normativa e delle prassi di gestione dei dati personali, ai sensi dell'art. 39 RGPD.

   Il RPD/DPO è incaricato dei seguenti compiti:

   a) informare e fornire consulenza al Titolare e ai Designati 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/DPO può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
   b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento.
   Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
   c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;
   d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD/DPO in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al 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/DPO.

2. Il Titolare ed il Responsabile del trattamento assicurano che il RPD/DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   - il RPD/DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti che abbiano per oggetto questioni inerenti la protezione dei dati personali;
   - il RPD/DPO 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/DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal RPD/DPO, è necessario motivare specificamente tale decisione;
   - il RPD/DPO deve essere consultato *tempestivamente* qualora si verifichi una violazione dei dati o un altro incidente.

3. Il RPD/DPO 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.

4. La figura di RPD/DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
   - il Titolare del trattamento;
   - il Responsabile del trattamento;
   - qualunque incarico o funzione che comporti la determinazione di finalità o mezzi del trattamento.

5. Il Titolare ed il Responsabile del trattamento forniscono al RPD/DPO le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare, è assicurato al RPD/DPO:
   - supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa, di bilancio, di Peg e di Piano della performance;
   - tempo sufficiente per l'espletamento dei compiti affidati al RPD/DPO;
   - supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD/DPO (formato dal RPD/DPO 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.

6. Il RPD/DPO 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/DPO non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti.
   Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD/DPO riferisce direttamente al Titolare - Sindaco o suo delegato - od al Responsabile del trattamento.
   Nel caso in cui siano rilevate dal RPD/DPO o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD/DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo formalmente al Titolare ed al Responsabile del trattamento.

Art.7 Sicurezza del trattamento

1. Il Comune di Forlì e ciascun Dirigente mette 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. Il Dirigente riesamina e aggiorna in modo periodico le misure, d'intesa con il Responsabile della transizione Digitale, sentito il Dirigente preposto alla sicurezza dei sistemi informativi e con il supporto del RPD/DPO. Tali aggiornamenti sono pubblicati sulla rete Intranet e illustrati nelle sessioni formative.

3. 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.

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

- 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. 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.

6. Il Comune di Forlì e ciascun Designato al trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

7. I nominativi ed i dati di contatto del Titolare e del Responsabile della Protezione Dati sono pubblicati sul sito istituzionale del Comune, *sezione* "Amministrazione trasparente", oltre che nella *sezione* "privacy" appositamente prevista.

8. Qualunque perdita, furto di dati personali deve essere tempestivamente segnalato e trattato, con le modalità previste dalla *procedura di gestione dei data breach*.

Art.8 Registri

1. Il Registro delle attività di trattamento è il registro dell'Ente che contiene le informazioni relative alle attività svolte da ciascun Servizio. Detto registro è predisposto e aggiornato costantemente dal Dirigente, relativamente alle banche dati degli ambiti di competenza, avvalendosi del Gruppo dei Referenti Privacy relativamente al popolamento dei trattamenti e dell'anagrafica dei responsabili esterni del trattamento (fornitori).

2. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto del Comune, del Sindaco e/o del suo Delegato ai sensi del precedente art.2, eventualmente del Contitolare del trattamento, del RPD/DPO;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.7.

3. 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.

4. Il Registro dei data breach è il registro dell'Ente ove il Dirigente provvede ad annotare le violazioni di dati personali che si sono verificate all'interno del Servizio, ma anche i data breach comunicati dai fornitori esterni, ai quali ha affidato servizi che implicano il trattamento di dati personali.

5. Entrambi i registri sono messi a disposizione dell'Autorità di controllo.

Art. 9 Estratto delle categorie di attività trattate

1. L'estratto delle categorie di attività trattate da ciascun Designato al trattamento di cui al precedente art. 4 riguarda i trattamenti svolti all'interno di un determinato servizio e reca le seguenti informazioni:
   a) le categorie di trattamenti effettuati da ciascun servizio: 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;
   b) la tipologia di dati personali trattati;
   c) le finalità di trattamento;
   d) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   e) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.7.

2. L'estratto del registro è tenuto dal Designato al trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea.

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 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 effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
   b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
   c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
   d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
   e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
   f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
   g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il

Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

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

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:

   a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
   b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
   c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
   d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

   Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. 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.

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 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 Esercizio dei diritti

1. Ogni persona può tutelare i propri dati personali, in primo luogo, esercitando i diritti previsti dagli articoli da 15 a 22 del GDPR.

2. Se ritiene che il trattamento dei dati personali non sia conforme alle disposizioni vigenti ovvero se la risposta ad un'istanza con cui esercita uno o più dei diritti di cui al comma 1 non perviene nei tempi indicati o non è soddisfacente, l'interessato può rivolgersi all'Autorità Giudiziaria o all'Autorità di controllo (Garante per la protezione dei dati personali), in quest'ultimo caso mediante un reclamo ai sensi dell'art. 77 del GDPR.

3. L'istanza può essere riferita a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali, comunque trattati, ed è presentata all'Ente, senza formalità (es. posta elettronica, lettera raccomandata, etc.), fatte salve le limitazioni di cui agli artt. 2-undecies e 2-duodecis del D.LGS 196/2003 e le altre limitazioni previste dalla legge.

4. L'istanza scritta è indirizzata al Titolare, tramite il RPD/DPO, o al Dirigente del Servizio dove sono trattati i dati. Qualora il trattamento coinvolga più Servizi, il Dirigente ricevente l'istanza ne dà comunicazione agli altri Dirigenti che detengono i dati personali dell'interessato.

5. Se il trattamento è effettuato da soggetti terzi per conto dell'Ente, sull'istanza è competente a rispondere il Dirigente che ha provveduto alla nomina del fornitore del servizio.

6. Il riscontro all'istanza presentata viene fornito entro 30 giorni dalla data di ricezione della stessa, anche nei casi di diniego.

7. Se le operazioni necessarie per il riscontro sono complesse o vi è una particolare e comprovata difficoltà, il termine dei 30 giorni può essere esteso fino a 60 giorni, non ulteriormente prorogabili. Di tale proroga viene data informazione all'interessato entro 20 giorni dalla ricezione dell'istanza.

8. L'interessato esercita i propri diritti attraverso opportune modalità gratuite e celeri. Il rilascio di documenti digitali e di copie digitali di documenti analogici è gratuito.

9. Solo nel caso in cui le istanze siano manifestamente infondate, eccessive o di carattere ripetitivo, può essere addebitabile un contributo spese ragionevole, il cui importo è fissato dall'Amministrazione, oppure il Dirigente può rifiutare di soddisfare la richiesta, dimostrandone il carattere manifestamente infondato, eccessivo o ripetitivo.

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.

Art.14 Entrata in vigore e pubblicità

1. Il presente regolamento sostituisce interamente il precedente approvato con deliberazione consiliare n.81 del 20 aprile 2009 e s.m.i., "Regolamenti in materia di partecipazione popolare, esercizio dei diritti di accesso ed informazione, tutela della riservatezza, Codice II" (artt. da 136 a 147) ed entra in vigore decorsi 15 giorni dalla data di sua pubblicazione all'albo pretorio on line.

GLOSSARIO REGOLAMENTO

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

- **Titolare del trattamento** l'autorità pubblica (il Comune o altro ente locale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.

- **Designato speciale al trattamento** il Dirigente individuato con decreto del Sindaco che tratta dati personali in virtù del principio di titolarità diffusa.

- **Responsabile esterno del trattamenti** il soggetto pubblico o privato che tratta dati per conto del titolare del trattamento in modalità esternalizzata.

- **Autorizzato al trattamento** il dipendente della struttura organizzativa del Comune, incaricato dal dirigente designato al trattamento, 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 impresa esterna, incaricati dal Titolare o dal Responsabile del trattamento.

- **Registro delle attività di trattamento** elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile esterno del trattamento secondo le rispettive competenze.

- **DPIA - Data Protection Impact Assessment**" - "**Valutazione d'impatto sulla protezione dei dati** 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.