COMUNE DI
REGGIO EMILIA

SISTEMA GESTIONALE DEL COMUNE DI REGGIO EMILIA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Indice

1. Indirizzi generali

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito “Regolamento”) detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni.
Per dare attuazione ai suddetti obblighi ed adempimenti, occorre rivedere l’assetto delle responsabilità tenuto conto della specifica organizzazione del Comune di Reggio Emilia.

Il regolamento europeo individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

- il **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- il **Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- il **Responsabile della protezione dei dati** (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;
- **le persone autorizzate al trattamento dei dati personali** sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di “terzo” di cui al n. 10 del comma 1 art. 4 del Regolamento e che nell’articolazione organizzativa del Comune di Reggio Emilia viene definita come **Incaricato del trattamento.**
- Ancorché non previsto dal Regolamento europeo, per esigenze organizzative interne al Comune di Reggio Emilia viene introdotta la figura del **Coordinatore del trattamento.**

Con il presente documento il Comune di Reggio Emilia definisce il proprio ambito di titolarità, individua le figure preposte all’attuazione degli adempimenti previsti dalla normativa, indica i compiti assegnati al DPO designato e definisce i criteri generali da rispettare nell’individuazione dei soggetti autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito delle responsabilità.

2. Il Titolare del trattamento

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è il Comune di Reggio Emilia cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Spetta pertanto in particolare al Comune di Reggio Emilia:

- adottare, nelle forme previste dal proprio ordinamento, gli interventi regolamentari e gli atti con valenza disciplinare e di pianificazione necessari all'adeguamento al Regolamento;
- designare il Responsabile della protezione dei dati - DPO;
- designare i Coordinatori quali soggetti preposti all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
- effettuare apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compresi i profili relativi alla sicurezza informatica, in collaborazione con il DPO designato;
- istruire i soggetti autorizzati al trattamento dei dati personali, in collaborazione con il DPO designato.

3. I Responsabili del trattamento

Sono designati Responsabili del trattamento di dati personali i soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del Titolare.
Pertanto, qualora occorra affidare un contratto comunque denominato comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Attesa la natura obbligatoria delle designazioni dei responsabili del trattamento, questa deve essere prevista all'interno di contratti, convenzioni, accordi e, in ogni caso, in costanza di formazione del rapporto contrattuale, in aderenza ai facsimile messi a disposizione dalla struttura competente in materia di privacy. In caso di contratti in essere è possibile designare i soggetti esterni quali Responsabili del trattamento con lettera di designazione integrativa del contratto stesso che dovrà essere firmata dal contraente per accettazione.

4. I Coordinatori del trattamento

Sono designati Coordinatori degli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dal Comune di Reggio Emilia in esecuzione del Regolamento europeo 670/2016 i Dirigenti dei Servizi dell'Ente, ciascuno per il proprio ambito di competenza così come definito dall'incarico dirigenziale conferito loro dal Sindaco.

Di seguito, sono indicati i compiti affidati ai Coordinatori:

a) verificare la legittimità dei trattamenti di dati personali effettuati dai servizi di riferimento;

b) disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;

c) adottare soluzioni di privacy by design e by default;

d) tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;

e) predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento;

f) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione, fatta in forma scritta ed inviata all'ufficio referente per la privacy di cui al punto 6, deve essere effettuata in aderenza alle indicazioni contenute nel presente documento ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;

g) predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa, su segnalazione del Titolare o del DPO;

h) provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;

i) disporre l'adozione dei provvedimenti imposti dal Garante;

j) collaborare con il DPO tramite l'ufficio privacy di cui al punto 6 al fine di consentire allo DPO l'esecuzione dei compiti e delle funzioni assegnate;

k) adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri Coordinatori, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;

l) designare i Responsabili del trattamento.

Al Dirigente competente in materia di privacy spettano inoltre:

- la sottoscrizione degli atti di notifica e di consultazione preventiva al Garante;
- la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

5. Gli Incaricati del trattamento

Sono autorizzati alle operazioni di trattamento dei dati i Coordinatori, che conformano i loro trattamenti alle policy dell'Ente in materia di protezione dei dati personali e alle istruzioni di seguito riportate:

- sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- sono accertati legittimità e correttezza dei trattamenti, verificando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Sono, altresì, autorizzati tutti i soggetti che effettuino operazioni di trattamento, dipendenti e collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare o dei Coordinatori. Tali soggetti, chiamati "Incaricati del trattamento" devono essere formalmente autorizzati dai Coordinatori i quali devono farsi carico di comunicare all'ufficio privacy di cui al punto 6 l'elenco dei soggetti autorizzati avendo cura di aggiornare l'elenco stesso ad ogni variazione.

L’autorizzazione formale avviene tramite individuazione nominativa (nome e cognome) delle persone fisiche ed occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare. La designazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento. Tali istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo alle policy del Comune di Reggio Emilia in materia di sicurezza informatica e protezione dei dati personali.
L’elenco completo degli incaricati privacy dell’Ente è tenuto aggiornato dall’ufficio referente per la privacy di cui al punto successivo.

6. L’ufficio referente per la privacy ed il gruppo dei referenti privacy

Costituisce attuazione dei principi di informazione e sensibilizzazione del Regolamento europeo 679/2016 l’individuazione di un ufficio referente per la privacy.

L’ufficio referente per la privacy ha i seguenti compiti:

- lo studio e l’approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti anche dalle nuove disposizioni normative in materia di protezione dei dati personali;
- fungere da punto di contatto con il DPO designato;
- fornire supporto ai Servizi dell’Ente per ogni questione inerente l’applicazione del Regolamento europeo 679/2016;
- coordinare le richieste di parere al DPO dei Coordinatori.

E’ altresì opportuna la creazione di un gruppo permanente di referenti privacy composto dall’insieme dei soggetti individuati dal Coordinatore di ogni Servizio (nel numero massimo di due persone per Servizio) che assicuri la circolazione costante delle informazioni all’interno dei Servizi sugli adempimenti continuativi obbligatori e necessari in materia di protezione dei dati personali.

7. Il Responsabile della Protezione dei dati (DPO)

Il “Regolamento (UE) 2016/679 prevede l’obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO).
Specificatamente, sono di seguito indicati i compiti del DPO in aderenza agli articoli 37 e seguenti

del suddetto regolamento, conformati alla precipua organizzazione dell'Ente:

- informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali;
- sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Ente in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- coopera con il Garante per la protezione dei dati personali;
- funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del Servizio ICT competente o ne richiede di specifiche;
- promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;
- partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'Ente;
- formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento.
- fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato di seguito.

8. Pareri del DPO

Il DPO fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture dell'Ente presentano nei casi di seguito indicati.

Pareri obbligatori

Devono essere obbligatoriamente richiesti pareri in ordine a:

- individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'Ente intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente, anche a seguito di incidenti di sicurezza o analisi dei rischi;
- adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;
- individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
- incidenti di sicurezza.

Pareri facoltativi

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:

- progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;
- valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento 2016/679;
- valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016;
- opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Le richieste di parere devono essere inviate all'indirizzo di posta elettronica **privacy@comune.re.it** specificando nell'oggetto della mail: "Richiesta di parere al DPO"

Possono presentare le richieste di parere i Coordinatori del trattamento dei dati.

9. Il Servizio ICT competente

Il Servizio competente in materia di sistemi informativi, ovvero di sicurezza informatica, svolge un ruolo di supporto al DPO in tema di risorse strumentali e di competenze.

Al fine di adeguare le funzioni assegnate con la designazione della nuova figura del DPO è necessario prevedere per il Servizio i compiti di seguito meglio specificati:

- individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente. Tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo obbligatorio del DPO, come ad esempio per la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e per la redazione ed aggiornamento dei disciplinari tecnici trasversali;

- condivide le evidenze dell'analisi dei rischi con il DPO, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;

- provvede, ogni qualvolta venga avvertito un problema di sicurezza a:

  - attivare le procedure per la gestione degli incidenti di sicurezza, assicurando la partecipazione del DPO;
  - individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO;
  - segnalare al Dirigente competente in materia di privacy le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali;

- promuove l'osservanza della normativa e delle policy dell'Ente in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del DPO e realizza le verifiche specifiche richieste dello stesso;
- collabora con l'ufficio dell'Ente preposto alla formazione del Personale sui temi in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all'interno della Ente, coordinandosi con le azioni promosse dal DPO.

Al Coordinatore Dirigente competente in materia di sistemi informativi spetta, inoltre:

- l'adozione di policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario;
- designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
- richiamare obbligatoriamente nei contratti di sviluppo e acquisizione di software e piattaforme, la policy in materia di privacy e sicurezza informatica, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del contratto.