MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (MOP)

Allegato F

PIAO 2026-2028

MODELLO ORGANIZZATIVO
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Sommario

1. INDIRIZZI GENERALI

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito anche solo “GDPR”) e il D.lgs. 196/2003 dettano 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.

Il GDPR 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 (DPO): figura prevista dagli artt. 37 e ss. del GDPR, 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 dell’art. 4, comma 1, del GDPR.

Con il presente documento il Comune di Ferrara **definisce** il proprio ambito di titolarità, **delega** ai Dirigenti della struttura comunale, ciascuno per il proprio ambito di competenza, l’attuazione degli adempimenti previsti dalla normativa, **indica** i compiti assegnati al Responsabile della Protezione dei Dati (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, come sintetizzato nello schema di seguito riportato.

2. IL TITOLARE

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

- adottare, nelle forme previste dal proprio ordinamento, gli interventi normativi eventualmente necessari;
- designare il Responsabile della protezione dei dati (DPO);
- designare i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
- effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il Responsabile della Protezione dei Dati (DPO) designato;
- istruire i soggetti autorizzati al trattamento dei dati personali.

3. I SOGGETTI DELEGATI ATTUATORI

Sono designati quali soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dall'Ente, in esecuzione del GDPR e delle policy interne e ciascuno per il proprio ambito di competenza, i Dirigenti di Servizio. Qualora la struttura organizzativa non preveda un Dirigente di Servizio, sarà designato quale Soggetto delegato attuatore il Dirigente di Settore.

Relativamente ai dati personali trasversali a più strutture, il Soggetto delegato attuatore designato sarà il Dirigente sotto la cui direzione e controllo è svolto il trattamento.

Di seguito, sono indicati i compiti affidati ai soggetti delegati attuatori:

A. trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
B. verificare la legittimità e correttezza dei trattamenti di dati personali effettuati dalla struttura di riferimento, avuto particolare riguardo ai rischi che gli stessi presentano e alla natura dei dati personali da proteggere;
C. disporre, in conseguenza alla verifica di cui alla lett. B), 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;
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 GDPR;
F. autorizzare i soggetti al compimento di 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 deve essere effettuata in aderenza alle indicazioni contenute nel presente documento e, 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;
H. provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti all'esercizio dei diritti previsti dalla normativa;
I. disporre l'adozione dei provvedimenti imposti dal Garante;

J. collaborare con il Responsabile della Protezione dei Dati (DPO) al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
K. adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri Soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;
L. individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
M. garantire al Responsabile del Servizio competente in materia di sistemi informativi e al Responsabile della Protezione dei Dati (DPO) i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
N. notificare e comunicare le violazioni dei dati personali ai sensi degli artt. 33 e 34 del GDPR.
O. designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
P. effettuare preventiva valutazione d'impatto ai sensi dell'art. 35 del GDPR, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
Q. consultare il Garante, in aderenza all'art. 36 del GDPR, nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;
R. designare i Responsabili del trattamento.

Nell'attuazione dei compiti sopraindicati i soggetti delegati possono acquisire il parere del Responsabile della Protezione dei Dati (DPO) nei casi e con le modalità specificate nel seguito.

Nell'organizzazione interna, viene individuato un dirigente competente in materia per l'adozione ed aggiornamento di policy in materia di privacy, il quale si coordina con il Dirigente competente in materia di sistemi informativi, che adotta ed aggiorna le policy sulla sicurezza informatica.

4. 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 incarico 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 negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale.

5. GLI INCARICATI

I trattamenti possono essere effettuati da dipendenti, collaboratori e soggetti che a qualsiasi titolo operano sotto la diretta autorità del Titolare o dei soggetti delegati. Tali soggetti (di seguito anche “incaricati”) devono essere formalmente autorizzati dai soggetti delegati attuatori cui fanno capo a livello organizzativo e provvedere tempestivamente all'aggiornamento delle autorizzazioni in caso di modifiche. Gli incaricati sono quindi designati:

- tramite individuazione nominativa (nome e cognome) delle persone fisiche. In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare;
- tramite assegnazione funzionale della persona fisica alla unità organizzativa di minori dimensioni, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.

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 dell’Ente in materia di sicurezza informatica e protezione dei dati personali.

6. IL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Sono di seguito indicati i compiti del Responsabile della Protezione dei Dati (DPO) in aderenza agli artt. 37 e ss. del GDPR, 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, con il supporto del gruppo dei referenti designati dalle strutture;
- 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 il Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR, 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 GDPR;
- fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato di seguito.

<u>Pareri obbligatori</u>

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 GDPR;
- 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 GDPR;
- 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.

Possono presentare le richieste di parere i soggetti delegati attuatori o i soggetti dagli stessi delegati in base ai principi generali relativi all'istituto della delega.

Nei casi in cui il Responsabile della Protezione dei Dati (DPO) esprima pareri non positivi, il soggetto delegato attuatore deve formalizzare, nelle medesime forme utilizzate dal Responsabile della Protezione dei Dati (DPO) per l'espressione del parere, le motivazioni che giustificano l'esecuzione dell'attività o l'implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal Responsabile della Protezione dei Dati (DPO).

I pareri espressi dal Responsabile della Protezione dei Dati (DPO) sono conservati agli atti del soggetto delegato.

7. IL SERVIZIO SISTEMI INFORMATIVI DEL COMUNE DI FERRARA

Il Servizio Sistemi Informativi competente in materia di sistemi informativi e di sicurezza informatica svolge un ruolo di supporto al Responsabile della Protezione dei Dati (DPO) in tema di risorse strumentali e di competenze e in particolare, per quanto riguarda i sistemi informativi:

- 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 Responsabile della Protezione dei Dati (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 Responsabile della Protezione dei Dati (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 la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del Responsabile della Protezione dei Dati (DPO);
  - » individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del Responsabile della Protezione dei Dati (DPO);
- promuove la formazione di tutto il personale del Comune di Ferrara in materia di sicurezza informatica e di utilizzo dell'intelligenza artificiale in ambito lavorativo, anche attraverso un piano di comunicazione e divulgazione all'interno del Comune di Ferrara, coordinandosi con le azioni promosse dal Responsabile della Protezione dei Dati (DPO).

8. ACCESSO CIVICO GENERALIZZATO E RUOLO RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il Responsabile della Protezione dei Dati (DPO), le strutture dell'Ente, e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.).

L'art. 5 del D.lgs. 33/2013 ss.mm.ii. ha introdotto l'istituto dell'accesso civico "generalizzato", che attribuisce a "chiunque" il "diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione". L'esercizio di tale diritto soggiace ai limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del d.lgs. n. 33/2013.

L'art. 5, c. 5, d.lgs. n. 33/2013 prevede che, per ciascuna domanda di accesso generalizzato, l'amministrazione debba verificare l'eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria.

Il Responsabile della Protezione dei Dati (DPO) funge da supporto alle strutture competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti alle richieste di accesso civico generalizzato.

Il Responsabile della Protezione dei Dati (DPO) funge altresì da supporto al R.P.C.T. nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali.

Il Responsabile della Protezione dei Dati (DPO), inoltre, su richiesta delle strutture, esprime proprio parere in ordine alla valutazione dell'eventuale pregiudizio che l'accesso 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 GDPR.

Il Responsabile della Protezione dei Dati (DPO), su richiesta delle strutture, formula il proprio parere, entro tre giorni, in ordine all'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. Sulla scorta di tale parere, le strutture competenti sulle singole richieste di accesso effettueranno

il bilanciamento tra gli interessi asseritamente lesi e la rilevanza dell’interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.