ALLEGATO A

MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DELLA PROVINCIA DI FERRARA

Indice

SEZIONE 1
INDIRIZZI GENERALI

1.1 Premesse

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, che abroga la direttiva 95/46/CE, (di seguito anche solo "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.

Le disposizioni del D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali", nonché i provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante"), allo stato continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa succitata. Si evidenzia che è previsto comunque l'adeguamento della normativa nazionale alle disposizioni del Regolamento.

Per dare attuazione ai suddetti obblighi ed adempimenti, occorre definire l'assetto organizzativo per governare i processi di gestione della privacy e l'ambito delle responsabilità, tenuto conto della specifica organizzazione della Provincia di Ferrara.

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;
- 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.

Con il presente documento la Provincia di Ferrara definisce il proprio ambito di titolarità, incarica il Segretario generale, i Dirigenti, il Servizio Informatico, Affari Istituzionali e il Comandante del Corpo di Polizia provinciale, ciascuno per il proprio ambito di competenza, per l'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, come riportato nel seguito.

1.2 Struttura organizzativa

La struttura organizzativa della Provincia di Ferrara è attualmente articolata in strutture dirigenziali di Settore, Posizioni Organizzative (P.O.), Unità Operative Complesse (U.O.C.) e Semplici (U.O.S.).

Allo stato la Dotazione organica è composta 167 dipendenti, di cui 4 Dirigenti di Settore (più un Responsabile Settore Bilancio in comando dal mese di gennaio 2018) e 9 Responsabili di Posizioni Organizzative (+ 1 Posizione Organizzativa in "distacco" dalla Regione).

SEZIONE 2
MODELLO ORGANIZZATIVO

2.1 Il titolare

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è la Provincia di Ferrara 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 all'Ente:

- adottare, nelle forme previste dal proprio ordinamento, gli interventi regolamentari necessari, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali oggetto di prossimo adeguamento al Regolamento;
- designare il Responsabile della protezione dei dati;
- designare i soggetti incaricati dell'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
- effettuare, a mezzo delle strutture competenti, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il DPO designato;
- istruire i soggetti autorizzati al trattamento dei dati personali.

2.2 I soggetti Coordinatori dell'attuazione del Regolamento

Sono designati quali soggetti Coordinatori rispetto all'attuazione degli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dalla Provincia di Ferrara in esecuzione del Regolamento (di seguito anche solo "Coordinatori"):

- il Segretario Generale;
- i Dirigenti, ciascuno per il proprio ambito di competenza
- Comandante della Polizia provinciale per l'ambito di stretta competenza del Corpo di Polizia Provinciale quale organo di Polizia Giudiziaria.

Relativamente ai trattamenti di dati personali trasversali a più settori si applica il criterio della prevalenza.

I compiti affidati ai Coordinatori sono i seguenti:

a) verificare la legittimità dei trattamenti di dati personali effettuati dal settore 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 il settore di competenza;
e) predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento, secondo i modelli "standard" di cui al punto 2.7.;

f) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito "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 ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali adottate dall'Ente;
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 l'esercizio dei diritti previsti dalla normativa;
i) disporre l'adozione dei provvedimenti imposti dal Garante;
j) collaborare con il 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 gli altri Coordinatori, 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 trasversali a più unità organizzative 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 Dirigente del servizio informatico e al 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. Devono inoltre fornire al Dirigente del Servizio Informatico i pareri per la gestione delle richieste di abilitazione all' accesso ai dati personali inerenti trattamenti di competenza di ciascun Dirigente da parte di altri soggetti;
n) designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
o) effettuare preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, 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;
p) consultare il Garante, in aderenza all'art. 36 del Regolamento e nelle modalità previste dal par. 3.1 lett b), 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;
q) richiamare obbligatoriamente nei contratti di sviluppo di software e piattaforme, la policy in materia di sviluppo delle applicazioni, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del contratto;
r) curare la designazione dei Responsabili esterni del trattamento di competenza del Titolare;
s) segnalare senza indugio al Titolare e al DPO eventuali incidenti di sicurezza che impattino su dati personali e curare, nei tempi richiesti, la predisposizione delle notifiche e comunicazioni obbligatorie al Garante e all'interessato, di competenza del Titolare, nei casi previsti dagli artt. 33 e 34 del Regolamento. Al riguardo verranno emanate specifiche policy.

Nell'attuazione dei compiti sopraindicati i Coordinatori possono acquisire il parere del DPO nei casi e con le modalità specificate nel seguito.

Fermo restando che la responsabilità delle attività sopraindicate rimane in ogni caso in capo al Coordinatore, in ragione del fatto che non sono ascrivibili a funzioni di direzione, coordinamento generale e controllo, sono eventualmente demandabili agli incaricati i compiti di cui alle d) e h).

2.3 I responsabili esterni 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, in aderenza ai fac-simili adottati dall'Ente.

2.4 Gli incaricati

Sono autorizzati al compimento alle operazioni di trattamento dei dati i Coordinatori di cui al paragrafo 2.2, ai sensi della presente disciplina, che conformano i loro trattamenti alle policy dell'Ente in materia di protezione dei dati personali e alle istruzioni di seguito riportate:

- devono trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- devono verificare 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 devono essere da questi formalmente autorizzati.

Gli incaricati sono quindi designati:

- 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
- tramite individuazione nominativa (nome e cognome). In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare.

Agli stessi possono essere eventualmente demandati i compiti di cui al paragrafo 2.2 lett. d) ed h).

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 di protezione dei dati personali.

2.5 Il Responsabile della Protezione dei dati (DPO)

Il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 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 37 e ss. 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, con il supporto dei Coordinatori;
- 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 informatico 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 la realizzazione del registro delle attività di trattamento di cui all'art. 30 del Regolamento;
- verifica la corretta tenuta dei Registri delle attività di trattamento
- fornisce i pareri obbligatori e facoltativi richiesti dai Coordinatori secondo quanto specificato di seguito.

2.6 Pareri del DPO

Il DPO fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che i Coordinatori presentano nei casi di seguito indicati.

2.6.1 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.

2.6.2 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 contro interessati, 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 contro interessati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la gravità del danno agli interessi degli opponenti.

Le richieste di parere saranno inviate al DPO a mezzo posta elettronica all' indirizzo che il DPO rende disponibile.

Possono presentare le richieste di parere i Coordinatori, così come individuati al paragrafo 2.2.

I pareri sono espressi nel rispetto delle seguenti codifiche:

- NC: acronimo di "non conformità", nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;
- OS: acronimo di "osservazione", nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;
- PO: acronimo di "positivo", nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy dell'Ente in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima parere "NC"" il Coordinatore deve formalizzare, nelle medesime forme utilizzate dal 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 DPO.

I pareri espressi dal DPO sono conservati agli atti. Il DPO è tenuto al segreto e o riservatezza in merito all' adempimento dei propri compiti.

2.7 Il Servizio Affari Istituzionali

Il Servizio Affari Istituzionali 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 seguenti compiti:

- Adotta modelli "standard" di informative e policy di tipo organizzativo a carattere generale/trasversale inerenti il trattamento dati personali;
- Diffonde il materiale di cui sopra e svolge verifiche sulla puntuale osservanza della normativa e delle policy dell'Ente in materia
- Promuove la formazione di tutto il personale dell'Ente in materia di privacy, anche attraverso un piano di comunicazione e divulgazione, coordinandosi con le azioni promosse dal DPO.
- Disciplina e regola gli orari e le modalità di accesso ai locali dell'Ente predisponendo le adeguate misure di sorveglianza ove necessario.
- Adegua gli strumenti regolamentari dell'Ente con il supporto del DPO
- Disciplina le modalità di funzionamento Gruppo dei Referenti Privacy
- Coadiuva il DPO nelle comunicazioni con il Titolare.

Nella fase iniziale di adeguamento alle disposizioni del Regolamento il Servizio Affari Istituzionali si avvarrà del gruppo di lavoro GDPR appositamente istituito dal Segretario Generale.

2.8 Il Servizio Informatico

Il Servizio informatico svolge anch'esso 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 seguenti compiti, attinenti unicamente l'utilizzo e la gestione degli strumenti informatici/telematici:

- individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informatizzato dell'Ente. Tutte le soluzioni informatiche 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 trattati con strumenti informatici e per la redazione ed aggiornamento dei disciplinari tecnici trasversali;
- condivide le evidenze dell'analisi dei rischi di matrice informatica 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 informatica relative a sistemi presidiati dal Servizio stesso (a titolo meramente esemplificativo sono escluse le notifiche inerenti lo smarrimento di cellulari, chiavette contenenti dati personali trattati dalla Provincia) a:
  - attivare la struttura cui sono demandati compiti relativi alla 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;
- curare nei tempi richiesti la predisposizione delle notifiche e comunicazioni obbligatorie al Garante e all'interessato nei casi previsti dagli artt. 33 e 34 del Regolamento, così come già esplicitato ai paragrafi precedenti.

- svolge le verifiche sulla puntuale osservanza della normativa e delle policy dell'Ente in materia di sicurezza informatica delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del DPO e realizza le verifiche specifiche richieste dello stesso;
- promuove la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione, coordinandosi con le azioni promosse dal DPO.

Al Dirigente del Servizio informatico spetta in particolare 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.

2.9 Il Gruppo dei Referenti Privacy

Costituisce attuazione dei principi di informazione e sensibilizzazione del Regolamento europeo n. 679/2016 la costituzione di un gruppo permanente di referenti privacy che assicuri un presidio per le strutture dell'Ente per quel che concerne gli adempimenti continuativi, lo studio e l'approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti anche delle nuove disposizioni normative.

Il Gruppo di referenti, formato da almeno un referente per Settore designato dal rispettivo Dirigente, ha i seguenti compiti:

- supportare le strutture del Settore di rispettiva appartenenza, al rispetto delle misure per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Ente, anche a seguito di analisi ed approfondimenti in seno al Gruppo stesso.
- effettuare, su impulso del Dirigente di riferimento, la ricognizione e l'aggiornamento costante del Registro dei trattamenti di dati personali effettuati del Settore di appartenenza;
- fornire al proprio responsabile ogni utile informazione raccolta nell'ambito dei trattamenti del Settore di riferimento inerente rischi e relative misure di contrasto volte alla protezione dei dati personali;
- diffondere nel Settore di appartenenza le buone prassi in materia di protezione dei dati personali.

Si demandano a future disposizioni le modalità di funzionamento del Gruppo.