COMUNE DI SANT'ILARIO DENZA

Provincia di Reggio Emilia

MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Approvato con deliberazione di G.C. n.3del 10/01/2019

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 e 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"), 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 rivedere l'assetto delle responsabilità tenuto conto della specifica organizzazione del Comune di Albinea.

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 l'Ente definisce il proprio ambito di titolarità, 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.

Il Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è l'Ente 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:

A. adottare, nelle forme previste dal proprio ordinamento, gli interventi normativi necessari, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali oggetto di prossimo adeguamento al Regolamento;

B. designare il Responsabile della protezione dei dati;

C. designare eventualmente i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;

D. 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 DPO designato;

E. verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;

F. 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;

G. adottare soluzioni di privacy by design e by default;

H. tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;

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

J. 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 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;

K. predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;

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

M. disporre l'adozione dei provvedimenti imposti dal Garante;

N. collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

O. 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;

P. 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;

Q. garantire al Responsabile del Servizio competente in materia di sistemi informativi 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;

R. designare gli amministratori di sistema in aderenza alle norme vigenti in materia;

S. 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;

T. 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;

U. 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;

V. designare i Responsabili del trattamento.

Nello svolgimento dei predetti compiti il Titolare del trattamento è coadiuvato dal Segretario generale. Relativamente ai trattamenti di dati personali trasversali a più strutture si applica il criterio della prevalenza.

2. Responsabili del trattamento dati

Ai fini dell'effettuazione del trattamento, in qualità di soggetti che presentano le garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate, sono individuati responsabili del trattamento i titolari di posizione organizzativa dell'Ente quali responsabili delle strutture apicali dello stesso. I trattamenti da parte del Responsabile del trattamento sono autorizzati e disciplinati dall'atto di incarico, in relazione ai profili funzionali di competenza di ciascuna articolazione organizzativa dell'Ente. Sono delegati ai titolari di posizione organizzativa in qualità di Responsabili del trattamento i compiti di cui alle lettere: E F G H J K L O P Q S U.

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

3. Responsabile competente in materia di sistemi informativi

Al Responsabile 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;

• 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.

4. Responsabili del trattamento esterni

Sono designati responsabili del trattamento di dati personali anche i soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, o altro atto comunque denominato, 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. Incaricati

Sono autorizzati al compimento alle operazioni di trattamento dei dati i soggetti delegati attuatori di cui al precedente paragrafo ed i soggetti da loro delegati ai sensi della presente disciplina, che conformano i loro trattamenti alle policy 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 verificati 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 Responsabili. Tali soggetti sono da questi formalmente autorizzati e 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, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità. In questo caso l'assegnazione tramite il PEG delle risorse umane alle singole articolazioni organizzative dell'ente equivale a formale designazione e autorizzazione al compimento delle operazioni di trattamento di competenza della singola articolazione organizzativa, salvo ove diversamente espressamente indicato. Le istruzioni impartite agli incaricati del trattamento, formulate per iscritto, 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. 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 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 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.

7. 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.

7.1 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 sicurezza.

7.2 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 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 dpo-team@lepida.it nelle modalità che saranno stabilite dall'Ente. Possono presentare le richieste di parere i soggetti delegati attuatori o i soggetti delegati in base ai principi generali relativi all'istituto della delega.

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 regionali in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima pareri "NC" e "OS" il soggetto delegato attuatore 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 del soggetto delegato.

8. 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 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;

◦ segnalare al Responsabile competente in materia di sistemi informativi le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali;

• svolge verifiche sulla puntuale 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;

• promuove la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all'interno della Ente, coordinandosi con le azioni promosse dal DPO.

9. Accesso civico generalizzato e ruolo DPO

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il DPO, le strutture dell'Ente e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.). Il D.L. 97/2016, di modifica del D.lgs. 33/2013, 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 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 le richieste di accesso civico generalizzato. Il 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 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 Regolamento UE n. 679/2016.

Il 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 lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.