Comune di Sestola
Provincia di Modena
C.so Umberto I, 5- 41029 Sestola (MO)
Tel 053661787 fax 053661787
comune@cert.comune.sestola.mo.it

MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Approvato con deliberazione di G.C. n. 66 del 26/05/2018

Sommario

Indirizzi generali

Il Regolamento (UE) 2016/679 del 27 Aprile 2016 approvato dal Parlamento Europeo e dal Consiglio (di seguito detto " Regolamento") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati abroga la direttiva 95/46/CE e 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 Sestola.

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 RPD): figura prevista dagli artt. 37 e ss. del Regolamento, che ne disciplinano la designazione, i compiti, le funzioni e le responsabilità;
- le persone, interne all'Ente autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare: 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 il Comune di Sestola definisce il proprio ambito di titolarità:
- delineando ai Responsabili di Area, titolari di Posizione Organizzativa, ciascuno per il proprio ambito di competenza, l'attuazione degli adempimenti previsti dalla normativa;
- indicando i compiti assegnati al RPD designato;
- definendo i criteri generali da rispettare nell'individuazione dei soggetti autorizzati a compiere le operazioni di trattamento dati;
- delineando il complessivo ambito delle responsabilità, come sintetizzato nello schema di seguito riportato.

Il Titolare

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è il Comune di Sestola, rappresentato dal Sindaco pro tempore, che è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del Regolamento: leicità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conversazione, integrità e riservatezza. A tal fine al Titolare spetta l'adozione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al Regolamento.
Spetta in particolare al Comune:

- 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;
- designare, con apposito Decreto, il Responsabile della Protezione dei Dati (RPD);
- nominare, con apposito Decreto di incarico, i soggetti interni all'Ente delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali (Responsabili Interni);
- designare l'Amministratore di Sistema in aderenza alle norme vigenti in materia;
- effettuare apposite verifiche sull'osservanza delle vigenti disposizioni in materia di trattamento dei dati , ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il RPD designato;
- istruire i soggetti autorizzati al trattamento dei dati personali.

I Responsabili interni

Sono designati Responsabili interni i soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dall'Ente in esecuzione del regolamento:

- Il Vice Segretario Comunale: con riferimento al ruolo di Responsabile della Prevenzione della Corruzione e della Trasparenza (R.P.C.T) del Comune di Sestola;
- I Responsabili di Area, titolari di Posizione Organizzativa: ciascuno per il proprio ambito di competenza e relativamente ai trattamenti di dati personali trasversali a più Aree si applica il criterio della prevalenza.

I Responsabili interni autorizzati, ai sensi della presente disciplina, 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 verificati la legittimità e la correttezza dei trattamenti, verificando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Di seguito, sono indicati i compiti affidati ai Responsabili interni:

a) verificare la legittimità dei trattamenti di dati personali effettuati dall'Area 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 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita);
d) tenere costantemente aggiornato il Registro delle Attività di Trattamento per l'Area di competenza;
e) predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento;
f) individuare, se necessario, nell'ambito della propria Area i soggetti autorizzati a compiere operazioni di trattamento (sub responsabili) 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 i sub responsabili, 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 RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni che gli sono state assegnate;
k) adottare, se necessario, specifici disciplinari tecnici di Area, anche congiuntamente con altri soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi all'ambito 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 sub responsabili o incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
m) garantire al responsabile incaricato in materia di sistemi informativi e al RPD 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) 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;

o) 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;
p) richiamare obbligatoriamente negli eventuali 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;
q) è responsabile della notifica e della comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

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

I sub responsabili e gli incaricati interni del trattamento

Fermo restando che la responsabilità delle attività indicate al paragrafo sopra rimane in ogni caso in capo ai Responsabili Interni, in ragione del fatto che non sono ascrivibili a funzioni di direzione, coordinamento generale e controllo, in base ai principi generali relativi all'istituto della delega, essi possono individuare sub responsabili del trattamento dei dati tra i collaboratori all'interno della propria Area di Competenza.
Possono, altresì, essere autorizzati al trattamento tutti i soggetti (definiti "incaricati") che effettuano operazioni di trattamento di dati, dipendenti e collaboratori a qualsiasi titolo, e che operano sotto la diretta autorità del Titolare o dei Responsabili interni.
I sub responsabili e gli incaricati devono essere formalmente individuati come segue:

- 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 all'unità organizzativa di minori dimensioni, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.

La designazione scritta deve inoltre contenere i compiti e le istruzioni impartite a ciascuno. Le 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 Sestola in materia di sicurezza informatica e protezione dei dati personali.

I Responsabili esterni del trattamento

Sono designati Responsabili Esterni 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 valutandone anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali, affinché lo stesso sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, 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.

Il Responsabile della Protezione dei dati (RPD)

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 (di seguito RPD).
Specificatamente, sono di seguito indicati i compiti del RPD in aderenza agli 37 e ss del suddetto Regolamento, conformati alla precipua organizzazione del Comune:

- informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con il supporto dei Responsabili interni del trattamento;
- sorveglia l'osservanza del Regolamento e della normativa in materia di protezione dei dati personali, fermo restando le responsabilità del Titolare del Trattamento dei Dati. 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 ed indirizzo nei confronti del Titolare;
- sorveglia sulle 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 e funge da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se necessario, consultazioni relativamente a qualunque altra questione;

- partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del servizio competente in materia di sistemi informativi 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;
- fornisce i pareri obbligatori e facoltativi richiesti dai Responsabili interni o dal Titolare.

Pareri del RPD

Il RPD fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che gli uffici 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 mitigare il rischio emerso dalle criticità sull'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
- incidenti 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 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita);
- valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento;
- 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;

- 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, per il successivo inoltro, all'indirizzo di posta elettronica comune@cert.comune.sestola.mo.it nelle modalità che saranno stabilite dall'Ente.

Possono presentare le richieste di parere i Responsabili Interni del trattamento 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 dell'Ente in materia di protezione dei dati personali.

Nei casi in cui il RPD esprima pareri "NC" e "OS" il Responsabile Interno che li ha richiesti deve formalizzare, nelle medesime forme utilizzate dal RPD 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 RPD.

I pareri espressi dal RPD sono conservati agli atti del Responsabile Interno che li ha richiesti.

Il Servizio ICT competente

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

Nel Comune di Sestola detto Servizio è affidato a soggetto esterno, non essendo presenti nell'organico le necessarie professionalità, con il coordinamento e controllo del Responsabile dell'Area Tecnica.

Al fine di adeguare le funzioni assegnate con la designazione della nuova figura del RPD, il Servizio si fa carico dei 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 RPD, 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 RPD, 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:
    - attivarsi per la gestione degli incidenti di sicurezza, assicurando la partecipazione del RPD;
    - individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del RPD;
    - segnalare al Responsabile dell'Area Tecnica le violazioni dei dati personali per l'avvio delle procedure finalizzate alla 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, ove necessario, la partecipazione del RPD e realizza le verifiche specifiche richieste dello stesso;
- collabora, su richiesta, alla formazione di tutto il personale dell'Ente in materia di sicurezza informatica, coordinandosi con le azioni promosse dal RPD.

Accesso civico generalizzato e ruolo del RPD

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il RPD, i Responsabili di Area 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 RPD funge da supporto ai Responsabili di Area 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 RPS 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 RPD, inoltre, su richiesta dei Responsabili di Area, 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.

Il RPD, su richiesta dei Responsabili di Area, 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 i Responsabili di Area 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.