## MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

### INDIRIZZI GENERALI

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio europeo 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. n. 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 dell'ASP "Giorgio Gasparini".

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 compiti, funzioni e responsabilità;
- **Persone autorizzate al trattamento** dei dati personali sotto l'autorità diretta del titolare o 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'ASP "Giorgio Gasparini" definisce il proprio ambito di titolarità, delega a Dirigenti e Incaricati di P.O., ciascuno per il proprio ambito di competenza, l'attuazione degli adempimenti previsti dalla normativa, indica i compiti assegnati al RPD 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.

### IL TITOLARE

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

- 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 il Responsabile della Protezione dei Dati;
- Designare i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;

- Effettuare, a mezzo dei servizi competenti, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compresi i profili relativi alla sicurezza informatica, in collaborazione con il RPD designato;
- Istruire i soggetti autorizzati al trattamento dei dati personali.

**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 regolamento il Direttore pro tempore, con funzioni di Coordinatore, e gli incaricati di Posizione Organizzativa, ciascuno per il proprio ambito di competenza. In assenza di incaricato di Posizione Organizzativa possono essere designati i coordinatori responsabili del servizio.

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

Di seguito sono indicati i compiti affidati al Coordinatore in materia di protezione dei dati personali, in persona del Direttore pro tempore dell'Ente:

a. Adottare soluzioni di privacy "by design" e "by default", ossia configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti dell'interessato, tenendo conto del contesto complessivo ove il trattamento si colloca ed i rischi per i diritti e le libertà dell'interessato;
b. Predisporre il modello di informativa relativo al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento;
c. Predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
d. Disporre l'adozione dei provvedimenti imposti dal Garante;
e. Collaborare con il RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnati;
f. Adottare, se necessario, specifici Disciplinari tecnici per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali;
g. Garantire al Responsabile dei 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;
h. Designare l'Amministratore di sistema in aderenza alle norme vigenti in materia;
i. Designare gli altri soggetti delegati attuatori nell'ambito degli incaricati di Posizione Organizzativa;
j. Effettuare la preventiva valutazione d'impatto ove necessaria ai sensi dell'art. 35 del Regolamento;
k. Consultare il Garante, in aderenza all'art. 36 del Regolamento nei casi in cui la valutazione d'impatto a norma dell'art. 35 indichi che il trattamento presenta un rischio residuale elevato;
l. Richiamare nei contratti di sviluppo di software e piattaforme, la policy in materia di sviluppo delle applicazioni, così come indicato nel Piano Triennale per l'Informatica, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del contratto;
m. Designare i Responsabili del trattamento.

Di seguito sono indicati i compiti affidati agli altri Soggetti attuatori, in persona degli Incaricati di Posizione Organizzativa o, in caso di assenza, i coordinatori:

A. Verificare la legittimità dei trattamenti di dati personali effettuati dal servizio/area di riferimento;
B. Disporre, in conseguenza della verifica di cui sopra alla lettera 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. Tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;

D. 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;
E. Provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;
F. 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.

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

**RESPONSABILE COMPETENTE IN MATERIA DI SISTEMI INFORMATIVI**

Al Responsabile competente in materia di sistemi informativi, individuato nel Responsabile dell'Area Amministrativa spetta:

- 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, ogniqualvolta l'evoluzione tecnica o normativa lo renda necessario;
- Segnalare al Titolare del trattamento, in persona dell'Amministratore Unico dell'ASP, e al Coordinatore delle attività, le violazioni dei dati personali ai fini della notifica ai sensi dell'art. 33 del Regolamento, al garante per la protezione dei dati personali.

**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 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.

**GLI INCARICATI**

Sono autorizzati al compimento delle operazioni dei dati i soggetti delegati attuatori di cui sopra che conformano i loro trattamenti alle policy aziendali 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 al compimento delle operazioni di trattamento dei dati tutti i soggetti, dipendenti e collaboratori a qualsiasi titolo, che operano sotto la diretta autorità del Titolare o dei soggetti delegati attuatori. Tali soggetti devono essere da questi formalmente autorizzati.

Gli incaricati sono quindi designati:

- Tramite individuazione nominativa 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 avere allegate le istruzioni impartite agli incaricati del trattamento.

**IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)**

Il Regolamento 679/2016 prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (RPD).

Sono di seguito indicati i compiti del RPD in aderenza agli artt. 37 e ss. del suddetto regolamento, conformati all'organizzazione dell'ASP "Giorgio Gasparini":

- 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 privacy dell'Ente;
- 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'art. 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- Partecipa allo svolgimento delle verifiche di sicurezza svolte da chi ha la responsabilità dei sistemi informativi o ne richiede di specifiche;
- Promuove e cura la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;
- Partecipa alla gestione conseguente ad eventuali 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 Servizi secondo quanto specificato di seguito.

**PARERI DEL RPD**

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

**Pareri obbligatori**

Devono essere obbligatoriamente richiesti pareri in ordine a:

- Individuazione delle misure che abbiano 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 relativi alla 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 ai principi della privacy by design e by default;
- Eventuale valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 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 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 al RPD per il tramite dei Referenti dell'ASP: la Responsabile dell'Area Amministrativa (attualmente Paola Covili all'indirizzo di posta elettronica covili.p@aspvignola.mo.it) o la Dr.ssa Claudia Bergonzini all'indirizzo di posta elettronica bergonzini.c@aspvignola.mo.it.

Possono presentare le richieste di parere i soggetti delegati attuatori e 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 riscontrati elementi valutati come conformi alla normativa e alle policy aziendali in materia di protezione dei dati personali.

Nei casi in cui il RPD esprima pareri "**NC**" e "**OS**" il soggetto delegato attuatore 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 soggetto delegato attuatore.

**IL SERVIZIO "SISTEMI INFORMATIVI"**

In merito a questo servizio si rammenta che ci si avvale di un affidamento di servizio all'esterno, ma la responsabilità del servizio è inserita nell'ambito dell'Area Amministrativa e dunque, affidata al Responsabile di suddetta Area.

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.

Al fine di adeguare le funzioni assegnate con la designazione della nuova figura del RPD il suddetto Servizio svolge 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 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:
    - Svolgere i compiti relativi alla 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 Titolare del trattamento, in persona dell'Amministratore Unico dell'ASP, e al Coordinatore 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;
- svolge verifiche sulla puntuale osservanza della normativa e delle policy aziendali in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del RPD e realizza le verifiche specifiche richieste dallo stesso;
- promuove l'informazione di tutto il personale dell'Ente in materia di sicurezza informatica, attraverso un piano di comunicazione e divulgazione all'interno dell'Ente, coordinandosi con le azioni promosse dal RPD.

**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, formato dal Direttore in veste di Coordinatore e dagli incaricati di Posizione Organizzativa, che assicuri un presidio per l'Ente per gli adempimenti continuativi, lo studio e l'approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti anche dalle nuove disposizioni normative.

Il Gruppo dei referenti ha i seguenti compiti:

- attuare, per le strutture di appartenenza, le misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Ente, anche a seguito ad analisi ed approfondimenti in seno al Gruppo dei referenti;
- coordinare il puntuale aggiornamento della designazione dell'Amministratore di Sistema e la costante verifica dei privilegi assegnati allo stesso;
- effettuare la ricognizione costante, a mezzo del Registro, dei trattamenti di dati personali effettuati dalle strutture di appartenenza, servendosi di risorse e competenze messe all'uopo a disposizione;
- fornire supporto alle verifiche di sicurezza svolte dal Servizio "Sistemi Informativi" e/o dal RPD;
- trasmettere per il tramite del Referente dell'Ente, le richieste di parere al RPD di propria afferenza nei casi e con le modalità previsti dal presente documento.

**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, le Strutture dell'Ente e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.).

Il D.Lgs. n. 97/2016, di modifica del D.Lgs. n. 33/2013, ha introdotto l'istituto dell'accesso civico "Generalizzato", che attribuisce a chiunque il "diritto di accedere ai dati, ai documenti e alle informazioni detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione".

L'esercizio di tale diritto soggiace a limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'art. 5 bis del D.Lgs. n. 33/2013.

L'art. 5, comma 5, del 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 Servizi 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 RPD 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 Servizi competenti, esprime 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 n. 679 del 2016.

Il RPD, su richiesta dei Servizi competenti, 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 Servizi 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.