Allegato "A" alla Delibera di G. C. n. 357 del 27/11/2018

COMUNE DI RIMINI

MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(Regolamento (UE) 2016/679)

1) INTRODUZIONE

1.a) Contesto normativo di riferimento.

Con il Regolamento generale sulla protezione dei dati personali (Regolamento (UE) 2016/679 *(General Data Protection Regulation - GDPR)* – di séguito indicato "GDPR" - l'Unione Europea ha inteso introdurre una disciplina finalizzata a rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini, sia all'interno che all'esterno dei confini dell'unione europea. Il testo, pubblicato sulla Gazzetta Ufficiale dell'unione Europea il 4 maggio 2016, è divenuto definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.
Il GDPR è parte del cosiddetto "Pacchetto protezione dati personali", l'insieme normativo che definisce un nuovo quadro comune in materia di tutela dei dati personali per tutti gli Stati membri dell'UE e comprende anche la Direttiva in materia di trattamento dati personali nei settori di prevenzione, contrasto e repressione dei crimini. Dal 25 maggio 2018 dunque, anche per gli enti locali, il GDPR è andato a sostituire la direttiva sulla protezione dei dati (ufficialmente Direttiva 95/46/EC) approvata nel 1995.
Nell'ambito del nuovo quadro normativo che la Commissione europea ha voluto delineare e al quale gli Stati membri devono conformarsi, l'Italia ha recepito i nuovi principi attraverso l'art. 13 della legge n. 163/2017[1], entrata in vigore il 21 novembre 2017, che ha attribuito al Governo la delega ad adottare (entro sei mesi) uno o più provvedimenti rivolti a:

- abrogare le disposizioni Decreto Legislativo n. 196/2003 (Codice Privacy) che siano in contrasto o comunque incompatibili con la nuova disciplina europea in tema di trattamento di dati personali e a modificarlo al fine di dare puntuale attuazione alle disposizioni del GDPR;
- valutare l'opportunità di avvalersi dei poteri specifici del Garante per la protezione dei dati personali (di séguito Garante Privacy) affinché adotti provvedimenti attuativi e integrativi volti al perseguimento delle finalità previste dal GDPR;
- adeguare l'attuale regime sanzionatorio, a livello, penale e amministrativo, alle disposizioni del GDPR, al fine di garantire la corretta osservanza della nuova normativa.

Con il decreto legislativo 10 agosto 2018, n.° 101 pubblicato sulla GURI del 4/9/2018 ed entrato in vigore il 19/9/2018, sono state approvate le "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento europeo (UE) 2016/679, relativo alla protezione delle persone fisiche con riferimento ai dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dati)"*. Con tale decreto legislativo, che, in parte abroga, modifica e novella profondamente il precedente decreto 196/2003, andando a costituire il nuovo "Codice Privacy", si completa il quadro della disciplina normativa nella materia in oggetto. 'E importante sottolineare che la disciplina nazionale **integra** quella europea e le disposizioni nazionali sono da ritenersi legittime in quanto e nella misura in cui:

- rientrino nelle materie rimesse dal GDPR al legislatore nazionale;
- il loro contenuto sia conforme alle disposizioni del GDPR;
- esse siano interpretate e applicate nel rispetto del Regolamento.

La normativa italiana e quella europea costituiscono, dunque, un ordinamento giuridico integrato e complesso, retto dal principio di supremazia della normativa europea su quella nazionale.

[1] Legge 25 ottobre 2017, n. 163 " Delega del Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea – Legge di delegazione europea 2016-2017"

Tra le disposizioni contenute nel D.Lgs.101/2018, sono di particolare interesse per gli enti locali quelle relative all'assetto organizzativo, che andando a colmare un vuoto aperto dal regolamento UE, sono andate sostanzialmente a recuperare soluzioni già presenti nel precedente decreto 196/2003, pur con alcune importanti differenze sul piano definitorio.

Del complesso normativo costituito dal Regolamento (UE) 2016/679 e dal nuovo "Codice Privacy" si è doverosamente tenuto conto nella stesura del presente modello organizzativo, pur nella consapevolezza che il percorso di attuazione delle nuove disposizioni comporterà un ulteriore impegnativo lavoro di adeguamento, in particolare di natura organizzativa e con riferimento al registro dei trattamenti, di cui si dirà in appresso.

Per poter più efficacemente affrontare questi delicati compiti, il Comune di Rimini ha deciso di affidare a Lepida spa, società in house della Regione Emilia Romagna e degli enti locali della Regione (riuniti nella Community Network dell'Emilia Romagna), i servizi di supporto per gli adempimenti e gli adeguamenti derivanti dal Regolamento in questione (cfr. Deliberazione della Giunta Comunale n. ° 132 del 17/05/2018 e determinazione dirigenziale n.° 1215 del 21.05.2018) ed ha designato la stessa società quale Responsabile protezione dati.

Per l'applicazione delle disposizioni del GDPR si fa altresì riferimento alle indicazioni e linee guida emanate in materia dal Garante della Protezione Dati Personali.

Le principali novità introdotte dal Regolamento Generale sulla protezione dei dati personali (GDPR), possono essere così sintetizzate:

- è introdotta la responsabilità diretta dei titolari del trattamento in merito al compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali;
- è definita la nuova categoria di dati personali (i c.d. dati sensibili di cui al precedente Codice Privacy);
- viene istituita la figura obbligatoria del Responsabile della Protezione dei Dati, incaricato di assicurare una gestione corretta dei dati personali negli enti. Tale figura può essere individuata tra il personale dipendente in organico, oppure è possibile procedere ad un affidamento all'esterno, in base a un contratto di servizi;
- viene introdotto il Registro delle attività del trattamento ove sono descritti i trattamenti effettuati e le procedura adottate dall'ente; il Registro dovrà contenere specifici dati indicati dal GDPR;
- viene richiesto agli enti l'obbligo, prima di procedere al trattamento, di effettuare una valutazione di impatto sulla protezione dei dati; tale adempimento è richiesto quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. (si pensi, ad esempio, ai dati ottenuti dalla sorveglianza di zone accessibili al pubblico).

Il Decreto legislativo 101/2018 ha altresì introdotto (a conferma di quanto previsto dal D.Lgs.196/2003) la possibilità che titolare e responsabile deleghino compiti e funzioni a persone fisiche che operano sotto la loro autorità e che, a tal fine, dovranno essere espressamente designate. Questi soggetti, per altro, non potranno più essere definiti come "responsabili" (termine che il GDPR, riserva, come si vedrà nel prosieguo, ad altre figure).

1.b) I soggetti individuati dal regolamento e loro compiti.

Il GDPR ridisegna, in particolare, il ruolo, i compiti e le responsabilità del Titolare e del responsabile del trattamento dei dati personali, in relazione ai nuovi principi e strumenti introdotti dallo stesso, e individua la nuova figura del Responsabile della protezione dei dati.

1.b.1 Il titolare

Il Titolare dei trattamenti di dati personali, ai sensi degli artt. nn.4, 7 e 24 del Regolamento, è l'Ente (nella persona del suo Legale rappresentante), 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 al Titolare:

- adottare, nelle forme previste dal proprio ordinamento, gli interventi necessari, anche con riferimento alle disposizioni del nuovo "Codice" per la protezione dei dati personali;
- designare il Responsabile della protezione dei dati;
- designare i soggetti ai quali è affidata l'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 dati designato;
- assicurare l'adeguata istruzione dei soggetti designati e autorizzati al trattamento dei dati personali.

1.b.2 Il Responsabile del trattamento dei dati personali

Per Responsabile del trattamento dei dati personali deve intendersi soltanto il Responsabile esterno, che agisce per conto del Titolare, dietro affidamento di prestazioni o servizi.

1.b.3 Responsabile protezione dati (RPD o DPO)

Il regolamento prevede l'obbligo per il Titolare del trattamento, ove questo sia effettuato da un'amministrazione pubblica, di designare un Responsabile della protezione dati. Il Responsabile protezione dati ha compiti di consulenza nei confronti del Titolare e dei soggetti designati o autorizzati al trattamento e di sorveglianza sull'osservanza del Regolamento (art. 37 GDPR); il responsabile protezione dati può essere un dipendente del Titolare oppure assolvere i suoi compiti in base ad un contratto di servizio.

2) Il MODELLO ORGANIZZATIVO DEL COMUNE DI RIMINI.

2.a Premessa

In applicazione della previgente disciplina, il Comune di Rimini si è dotato dei seguenti atti organizzativi:

- Direttiva del Sindaco prot. n. 110238 del 17/06/2004 "Definizioni e nozioni preliminari per l'applicazione del "Codice in materia di protezione dei dati personali" (D.Lgs. 196/2003) e disposizione Sindacale di nomina dei dirigenti "responsabili di trattamento" concernente misure organizzative comuni a tutti i tipi di trattamento e misure di sicurezza relative ai supporti non informatici ;
- "Regolamento per il trattamento dei dati sensibili e giudiziari adottato con Delibera di Consiglio Comunale n. 168 del 15/12/2005;
- Documento Programmatico sulla Sicurezza, prot. n. 44153 del 30/03/2012.

Il presente modello organizzativo viene adottato nelle more dell'analisi di *set up* della organizzazione vigente, che dovrà essere compiuta in collaborazione con Lepida spa, e sarà pertanto soggetto agli adeguamenti conseguenti all'esito di tale attività.

2.b I Soggetti

2.b.a. Il Titolare.

Il Sindaco, in quanto legale rappresentante dell' Ente, riveste la figura di Titolare del trattamento.

Il Sindaco designa i dirigenti, ciascuno per il proprio ambito di competenza, quali soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti dei dati personali effettuati dall'Ente in esecuzione del regolamento e del "Codice".

Relativamente ai trattamenti dei dati personali gestiti da più strutture in modo trasversale, si applica il criterio della prevalenza.

Il Sindaco designa altresì il Responsabile della protezione dati. A questo adempimento ha provveduto con nota prot. n.° 2018 - 0144921 in data 22/5/2018 individuandolo in Lepida spa , società in house dell'Emilia Romagna e degli Enti locali della Regione (riuniti nella Community network dell'Emilia Romagna).

Per assicurare un'efficace attività di adeguamento alle disposizioni del GDPR, con deliberazione della Giunta Comunale n.° 132 del 17/05/2018 e successiva determinazione dirigenziale n.° 1215 del 21/05/2018, il Comune di Rimini ha altresì deciso di affidare a Lepida spa i servizi di supporto agli adempimenti in materia.

2.b.b.Personale dirigente

Sulla base del vigente assetto organizzativo-direzionale dell'Ente, al personale dirigente sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle nuove norme in materia di privacy, in coerenza con la previsione dell'art. 107 del D.Lgs. 267/2000. Con l'atto di incarico, il Sindaco attribuisce ai dirigenti i compiti e le funzioni connessi al trattamento dei dati. Ai dirigenti designati, in relazione all'ambito organizzativo di competenza, sono assegnati i seguenti compiti:

A. verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura 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[2];
D. implementare e 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 Regolamento;
F. individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati,

[2] Con l'espressione inglese "data protection by default and by design", si intende la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

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;

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 RPD/ 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 Dirigenti e/o Responsabili del trattamento, 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 Dirigente 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;
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, ai sensi dell'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. designare i Responsabili del trattamento.

Con atto in data 28/05/2018 n. 150905 il Sindaco ha disposto di confermare in capo ai Dirigenti del Comune di Rimini la responsabilità del trattamento dei dati anche successivamente all'entrata in vigore del Regolamento (UE) 2016/679.
I successivi provvedimenti di incarico dirigenziale dovranno recare apposita designazione dei dirigenti stessi quali soggetti attuatori delle disposizioni in materia.

2.b.c. Soggetti autorizzati ("incaricati")

I Dirigenti, fermo restando che la responsabilità delle attività elencate al punto precedente resta in capo ai medesimi, possono autorizzare per specifiche attività di trattamento dipendenti appartenenti alla struttura organizzativa di competenza; le operazioni di trattamento dovranno essere effettuate solo da soggetti formalmente autorizzati, che operano sotto la diretta autorità del Dirigente, attenendosi alle istruzioni impartire per iscritto, che individuano specificatamente l'ambito del trattamento consentito.
L'autorizzazione resta efficace sino a revoca formalmente adottata o fino al trasferimento dell'incaricato a struttura organizzativa di competenza di altro dirigente.

L'autorizzazione deve contenere:

- l'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;
- l'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.
Il presente documento verrà successivamente integrato con un modello di atto di autorizzazione.

2.b.d. I Responsabili del Trattamento

Sono designati Responsabili del trattamento di dati personali i soggetti esterni all'amministrazione che siano tenuti, a séguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamento 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 tramite inserimento nei diversi modelli contrattuali di apposite clausole vincolanti in ordine al rispetto delle disposizioni e degli obblighi in materia di protezione dei dati personali, in aderenza ai fac-simili che verranno adottati ad integrazione del presente atto.
I Responsabili del trattamento possono nominare dei sub-responsabili, purché autorizzati preventivamente. In tal caso il Responsabile vincola il sub-responsabile con un contratto (o altro atto giuridico conforme del diritto nazionale) che contenga gli stessi obblighi previsti nel contratto tra il Responsabile e l'Ente. Il responsabile iniziale conserva nei confronti dell'Ente l'intera responsabilità degli adempimenti degli obblighi del sub-responsabile.

2.b.e. Responsabile della Protezione Dati (RPD o Data Protection Officer - DPO)

Con provvedimento del Sindaco prot. n.° 2018 - 0144921 in data 22/5/2018, Lepida spa è stata designata quale "Responsabile protezione dati" ai sensi del Regolamento. I relativi dati di contatto sono stati comunicati al Garante per la protezione dei dati personali e sono pubblicati sul sito internet dell'Ente.
Sono di seguito indicati i compiti del DPO in aderenza agli artt. 37 e s.s. del suddetto regolamento, conformati all' 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.

2.b.f Struttura competente in materia di sistemi informativi.

Spetta alla struttura competente in materia di sistemi informativi 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; svolge, altresì, un ruolo di supporto al DPO in tema di risorse strumentali e di competenze.
La struttura è tenuta a mettere in atto tutte le misure adeguate, tecniche ed organizzative, per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto dei principi di *accountability*, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi, da esibire in caso di eventuali attività ispettive da parte degli organi competenti o di sorveglianza sulla conformità al GDPR da parte del DPO.

In particolare

- 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, la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e l' 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 tempestivamente al DPO 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 di 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 dell'Ente, coordinandosi con le azioni promosse dal DPO.

Al Dirigente competente in materia di sistemi informativi spetta:

- 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.

2.c I Processi e gli Strumenti

2.c.a. Il Registro delle attività di trattamento

In vigenza del precedente ordinamento questa Amministrazione si era dotata di atti di rilevazione dei processi e degli strumenti di gestione, con indicazione degli strumenti utilizzati e degli interventi operativi necessari.
Il Regolamento prevede l'adozione di un "registro delle attività di trattamento", che reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto del Comune, del Sindaco e/o del Dirigente designato, del RPD;
b) le finalità del trattamento;
c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Il registro rappresenta l'elemento centrale per la *governance* del modello di gestione privacy e va tenuto in forma scritta, anche in formato elettronico.
La tenuta del registro in formato elettronico, redatto sulla base di apposito schema predisposto da Lepida spa ed unico per tutto l'Ente, è affidata al Dirigente specificamente designato dal Sindaco, il quale coordina le attività di implementazione e aggiornamento sistematico dei dati del registro ad opera dei singoli dirigenti, a quali spetta la responsabilità sulla completezza e adeguatezza dei dati e delle misure indicati.

2.c.b. Il ruolo del Responsabile Protezione Dati- Pareri

Il Responsabile protezione dati 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.

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.

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 del D.Lgs. 14 marzo 2013, n. 33 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 agli indirizzi di posta elettronica: certificata segreteria@pec.lepida.it, e posta ordinaria dpo-team@lepida.it, per conoscenza al dirigente incaricato della tenuta del registro e al dirigente della struttura competente in materia di sistemi informativi.
Possono presentare le richieste di parere i Dirigenti designati relativamente alla disciplina di trattamento dati nelle materie di rispettiva competenza.
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 Dirigente 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 della struttura dirigenziale che ne ha fatto richiesta.

2.c.c. Gruppo Referenti Privacy

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

Il Gruppo di referenti è composto da 2 dipendenti per ciascun dipartimento o struttura ad esso equiparata designati dal relativo responsabile, dal responsabile dell'unita operativa CED o suo delegato, da un dipendente dell'ufficio Segreteria Generale incaricato della gestione dell'accesso civico ed è presieduto dal Dirigente responsabile dei servizi informativi.

Il Gruppo di referenti ha i seguenti compiti:

- collaborare con i dirigenti del dipartimento/struttura di appartenenza all'attuazione delle misure adeguate ed efficaci 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 dei referenti privacy;
- coordinare il puntuale aggiornamento delle designazioni degli amministratori di sistema all'interno dei dipartimenti/strutture di appartenenza e la costante verifica dei privilegi assegnati agli amministratori già designati;
- effettuare la ricognizione costante, a mezzo del Registro, dei trattamenti di dati personali effettuati dal dipartimento/struttura di appartenenza;
- fornire supporto alle verifiche di sicurezza svolte dal Servizio ICT e/o dal DPO;
- promuovere e collaborare alla revisione e all'aggiornamento dei Disciplinari Tecnici;
- coordinare le richieste di parere al DPO dei dirigenti del dipartimento/struttura di appartenenza nei casi e con le modalità previsti dal presente documento.

2.c.d. 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 2016/679.
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 asseritamente lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.

2.c.e. Monitoraggio

Come già sopra specificato, il presente modello organizzativo viene adottato nelle more dell'analisi di *set up* della organizzazione vigente, che dovrà essere compiuta in collaborazione con Lepida spa, e sarà pertanto soggetto agli adeguamenti conseguenti all'esito di tale attività. In tale occasione verrà altresì integrato con gli schemi di atti di designazione, autorizzazione, delega, ecc. citati nel testo.
Fino a tale momento restano validi gli atti e i provvedimenti organizzativi adottati, non specificamente modificati dal presente documento.
Anche a regime, il modello di gestione della privacy adottato dall'Ente dovrà essere sottoposto a costante monitoraggio da parte dell'Amministrazione, allo scopo di intervenire rapidamente, anche su proposta del DPO, sull'assetto organizzativo in caso di modifiche normative o a séguito dell'evoluzione tecnologica o della necessità di introdurre nuove e più efficaci politiche di gestione dei dati personali.