



DELIBERAZIONE N. 2018 - 34

**OGGETTO:** 2 PRIMI ADEMPIMENTI IN ATTUAZIONE DEL REGOLAMENTO UE 2016/679 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (GDPR).

Reggio Emilia, questo giorno 25 (venticinque) del mese di maggio dell'anno 2018 nella sede dell'Azienda in Via Pietro Marani 9/1 Reggio Emilia

### **IL CONSIGLIO DI AMMINISTRAZIONE**

nominato con deliberazione dell'Assemblea dei Soci dell' ASP "REGGIO EMILIA – Città delle Persone" n. 2016/3 del 11/01/2016, si è riunito alle ore            a seguito invito del Signor Presidente, con l'intervento dei Signori:

<b>N.</b>	<b>Componenti</b>	<b>Carica</b>	<b>Presenti</b>	<b>Assenti</b>
1	RAFFAELE LEONI	Presidente		

Assistono alla seduta il Direttore dell'Azienda: Maria Teresa Guarnieri  
e il segretario verbalizzante: Anna Maria Lacala

Il Presidente RAFFAELE LEONI assume la presidenza e, riscontrato legale il numero dei presenti per deliberare validamente, dichiara aperta la seduta.

PRIMI ADEMPIMENTI IN ATTUAZIONE DEL REGOLAMENTO UE 2016/679 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (GDPR).

**IL CONSIGLIO DI AMMINISTRAZIONE**

PREMESSO CHE:

- il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE, (GDPR), troverà piena applicazione dal 25/05/2018;
- con Legge 25 ottobre 2017 n. 163 recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea-Legge di delegazione europea 2016/2017, il Governo è stato delegato all'emanazione di uno o più decreti legislativi al fine di adeguare la normativa nazionale al suddetto Regolamento;
- il Consiglio dei Ministri, in data 21/03/2018, ha approvato in via preliminare uno schema di decreto legislativo sul quale ha acquisito il parere del Garante e che ha ora sottoposto all'esame della competente Commissione parlamentare;
- lo schema del decreto, nel testo attualmente consultabile, prevede l'abrogazione delle disposizioni del codice in materia di protezione dei dati personali, di cui al Decreto legislativo 30 giugno 2003 n. 196, incompatibili con il Regolamento UE e l' introduzione di nuove disposizioni, ovvero la modifica di altre;

CONSIDERATO CHE il Regolamento introduce significativi cambiamenti all'attuale quadro normativo e in particolare:

- il principio di *accountability*, ovvero responsabilizzazione, che pone in capo al titolare o, in sua vece, al responsabile del trattamento, il compito di adottare comportamenti attivi e tali da dimostrare la concreta adozione di misure idonee finalizzate ad assicurare l'applicazione del Regolamento e a garantire che il trattamento avvenga nel rispetto dei dettami normativi e senza rischio per le libertà e i diritti dell'interessato;
- i principi di "privacy by design" e di "privacy by default", ovvero la necessità di configurare il trattamento prevedendo sin 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 e i rischi per i diritti e le libertà dell'interessato;
- l'obbligo di notifica delle violazioni dei dati personali dalle quali derivino rischi per i diritti e le libertà degli interessati;

- l’obbligo per alcuni titolari di tenere un registro delle operazioni di trattamento, allo scopo di disporre di un quadro aggiornato dei trattamenti in essere, da esibire su richiesta al Garante, e di effettuare una valutazione d’impatto sulla protezione dei dati (DPIA);
- l’obbligo per alcuni titolari di designare un “Responsabile della protezione dei dati” (RPD), altrimenti detto “Data Protection Officer” (DPO), che disponga delle caratteristiche soggettive e oggettive richieste dal Regolamento (indipendenza, autorevolezza ecc.);

PRESO ATTO CHE il Regolamento pone in capo agli Enti pubblici adempimenti e attività impegnative, in virtù delle particolari categorie di dati che gli stessi trattano e che pertanto risulta necessario assicurare il corretto svolgimento del processo di adeguamento, coordinandolo con gli altri adempimenti, previsti dalla normativa vigente;

CHE il predetto Regolamento prevede l’obbligo per il titolare o il responsabile del trattamento di designare il RPD/DPO quando il trattamento è effettuato da un’autorità pubblica o da organismo pubblico (art. 37 paragrafo 1 lett. a);

CHE le predette disposizioni prevedono che il RPD/DPO “può essere un dipendente del titolare del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi” e deve essere individuato “in funzione delle qualità professionali, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione di dati e della capacità di assolvere i compiti di cui all’art. 39” e “il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile di trattamento”;

CHE la funzione di RPD/DPO è incompatibile con quelle di responsabile dei sistemi informativi dell’Azienda e di Responsabile di Prevenzione della Corruzione e della Trasparenza;

RILEVATO CHE l’Azienda è tenuta alla designazione obbligatoria del Responsabile Protezione Dati Personali nei termini previsti rientrando nella fattispecie prevista dall’art. 37 paragrafo 1 lett. a;

DATO ATTO CHE all’interno dell’Azienda non si ravvisano soggetti in possesso delle competenze richieste dall’art. 37 comma 5 del Regolamento;

CHE si ritiene quindi necessario reperire la necessaria professionalità in una figura esterna all’Azienda, con le caratteristiche soggettive e oggettive richieste;

ATTESO CHE le disposizioni prevedono la possibilità che un unico Responsabile della Protezione dei Dati possa essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione (art. 37 paragrafo 3 GDPR);

CONSIDERATO CHE:

- l'Azienda ha aderito alla Società LEPIDA S.p.A. mediante la sottoscrizione di un'azione del valore nominale di Euro 1.000,00 della società stessa, giusta deliberazione del Consiglio di Amministrazione n. 2017/8 del 28/02/2017, ratificata con deliberazione dell'Assemblea dei Soci n. 2017/5 del 23/06/2017;
- Lepida S.p.a. ha predisposto servizi di supporto per gli adempimenti e adeguamenti derivanti dal Regolamento Europeo 2016/679/UE per la protezione dei dati personali (GDPR) per tutti gli Enti della Regione Emilia-Romagna che sono stati approvati dal Comitato Permanente di Indirizzo e Coordinamento con gli Enti locali, istituito con la Legge Regionale n.11/2004 e successive modifiche e integrazioni, quale organismo della Community Network dell'Emilia-Romagna facente parte dell'Agenda Digitale dell'Emilia Romagna;
- tali servizi sono frutto dell'analisi, della progettazione e realizzazione condivisa tra Lepida S.p.A. e il sistema delle Comunità tematiche regionali, il quale ha come ulteriore obiettivo l'omogeneizzazione e la standardizzazione dei processi/procedimenti e dei trattamenti a livello regionale;
- con determinazione del Direttore n. 163 del 10/05/2018 l'Azienda ha aderito ai servizi GDPR di Lepida S.p.A. con l'obiettivo di promuovere, unitamente ad altre ASP della Provincia e della Regione, anche la standardizzazione dei processi/procedimenti e dei trattamenti dei dati delle diverse Asp operanti sul territorio regionale;
- tale impegno è stato ottenuto da Lepida S.p.A. per il tramite del Coordinamento Regionale dell'Associazione CISPEL, cui l'Azienda unitamente ad altre Asp aderisce, che ha richiesto la disponibilità ad individuare un unico referente RDP/DPO per le ASP che operano in contesti territoriali vicini;

ATTESO CHE il servizio di supporto per lo svolgimento degli adempimenti previsti dal GDPR fornito da Lepida S.p.A. comprende:

- il supporto per la verifica del rispetto dei principi fondamentali, della liceità del trattamento e delle misure a protezione dei dati, in modo da assicurare la conformità dei trattamenti al GDPR;
- la funzione di Responsabile della protezione dei dati (RPD/DPO);
- la messa a disposizione di uno strumento per il registro dei trattamenti (RecordeER);

VALUTATO, ai sensi dell'art. 37 paragrafo 3 del Regolamento, di procedere alla nomina condivisa di uno stesso Responsabile della Protezione dei Dati Personali (RDP/DPO) con gli Enti della Community network della Regione Emilia Romagna e le altre ASP del territorio provinciale e regionale, sulla base delle valutazioni condotte nelle sedi delle Comunità tematiche, anche in termini di affinità tra le relative strutture organizzative, funzioni (attività) e trattamenti di

dati personali, oltre che di razionalizzazione della spesa;

RITENUTO CHE Lepida SpA possa disporre al proprio interno del livello di conoscenza specialistica e delle competenze richieste dall'art. 37 par. 5 del GDPR per la nomina del DPO e non si trovi in situazioni di conflitto di interesse con la posizione da ricoprire, i compiti e le funzioni da espletare;

DATO ATTO CHE, con nota in atti al n. 5933 del 23/05/2018, Lepida SpA ha comunicato il nominativo del referente da inserire nella comunicazione di nomina del RPD/DPO al Garante, individuandolo all'interno del proprio team nella persona di Sergio Duretti;

CHE, con la medesima comunicazione, Lepida SpA ha trasmesso uno schema per l'adozione del modello organizzativo aziendale per la gestione degli adempimenti relativi alla normativa in materia di protezione dei dati personali, ove prevedere una più puntuale specificazione dei compiti assegnati al RPD/DPO e la sua interazione con le strutture interne, nonché uno schema di modello di informativa da adottare;

RITENUTO pertanto:

- di designare Lepida S.p.A. come RPD/DPO per l'Azienda, dando atto che il nominativo del referente individuato è quello di Sergio Duretti e, per effetto di quanto sopra, di autorizzare il Presidente, in qualità di rappresentante legale dell'Azienda, titolare del trattamento, a formalizzare la procedura di comunicazione dei dati di contatto del Responsabile della Protezione dei Dati (RPD /DPO) al Garante;
- di rinviare l'approvazione del modello organizzativo in materia di protezione dei dati personali a successivo atto, a seguito dell'effettuazione delle necessarie valutazioni organizzative e della valutazione dei rischi da effettuare con il supporto del RPD/DPO;
- di integrare le informative per gli utenti, i lavoratori/collaboratori, i fornitori, i locatari/conducenti di immobili aziendali con i dati obbligatori previsti dal Regolamento 679/2016 negli schemi allegati al presente atto a costituirne parte integrante e sostanziale ( All.1-5), fatta salva ogni ulteriore modifica a seguito di verifica congiunta condotta con il referente incaricato da Lepida S.p.A.;

DATO ATTO CHE

- i dati di contatto del Responsabile della Protezione dei Dati Personali (RPD/DPO) saranno indicati nell'informativa redatta ai sensi dell'art. 13 del GDPR e pubblicati sul sito istituzionale dell'Azienda;
- il Responsabile della Protezione dei Dati personali è incaricato, nel rispetto di quanto previsto dall'art. 39 par. 1 del GDPR, di svolgere in piena autonomia e indipendenza i seguenti compiti

e funzioni:

- a. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- b. sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati, nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del GDPR;
- d. cooperare con il Garante per la protezione dei dati personali;
- e. fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

DATO ATTO ALTRESÌ

CHE Lepida S.p.A. fornirà uno strumento informatico dalla medesima realizzato per la gestione del registro dei trattamenti e garantirà il supporto al titolare nell'analisi dei rischi e nell'individuazione delle relative misure di sicurezza;

CHE, con nota iscritta al P.G. al n. 5647 del 21/05/2018, Lepida S.p.A. ha comunicato che elaborerà una bozza di possibile politica e procedura per la gestione degli incidenti di sicurezza ed eventualmente la notifica del *data breach*;

RITENUTO in via provvisoria, in attesa di implementare il lavoro con Lepida S.p.A.:

- di approvare il registro del trattamento dei dati personali allegato al presente atto quale parte integrante e sostanziale dello stesso (Allegato 6), dando atto che esso costituisce la prima base di lavoro su cui impostare l'attività con il referente di Lepida S.p.A.;
- di rinviare a successivo atto l'approvazione del documento di valutazione dei rischi e della procedura prevista in caso di violazione dei dati di cui all'art. 33 del GDPR, ad esito del confronto con Lepida S.p.A., previsto dal relativo contratto di servizio;

DATO ATTO CHE, in attesa della formalizzazione della procedura per la gestione degli incidenti di sicurezza e la notifica del *data breach*, si individua in via provvisoria, nel Direttore o suo delegato, la figura incaricata di effettuare la segnalazione al Garante della Privacy, ai sensi dell'art. 33 del GDPR;

RICHIAMATO l'art. 28 dello Statuto aziendale sulla validità e sullo svolgimento delle sedute che prevede, al comma 3, che il Consiglio deliberi a maggioranza assoluta dei votanti, prevalendo in caso di parità, il voto del Presidente e, al comma 5, che l'espressione del voto avvenga in forma palese, fatti salvi i casi in cui si tratti di questioni concernenti persone;

*Si procede alla votazione in forma palese della presente deliberazione e il Consiglio di Amministrazione all'unanimità dei presenti*

### **DELIBERA**

*per le motivazioni espresse in premessa e qui integralmente richiamate*

1. di avvalersi, della facoltà prevista dall'art. 37 paragrafo 3 del Regolamento UE n. 2016/679 (GDPR), di procedere alla nomina condivisa di uno stesso Responsabile per la protezione dei dati personali (RPD/DPO), con gli Enti della Community network della Regione Emilia Romagna e le altre ASP del territorio provinciale e regionale, attraverso Lepida S.p.A., sulla base delle valutazioni condotte nelle sedi delle Comunità tematiche, nonché delle ulteriori valutazioni condotte in sede di Coordinamento Regionale dell'Associazione CISPEL tra le varie Asp del territorio regionale;
2. di designare Lepida S.p.A. come RPD/DPO per l'Azienda, dando atto che il nominativo del referente individuato è quello di Sergio Duretti e, per effetto di quanto sopra, di autorizzare il Presidente, in qualità di rappresentante legale dell'Azienda, titolare del trattamento, a formalizzare la procedura di comunicazione dei dati di contatto del Responsabile della Protezione dei Dati (RPD/DPO) al Garante;
3. di rinviare l'approvazione del modello organizzativo in materia di protezione dei dati personali a successivo atto, a seguito dell'effettuazione delle necessarie valutazioni organizzative e della valutazione dei rischi da effettuare con il supporto del RPD/DPO;
4. di integrare le informative per gli utenti, i lavoratori/collaboratori, i fornitori, i locatari/conducenti di immobili aziendali con i dati obbligatori previsti dal Regolamento 679/2016 negli schemi allegati al presente atto a costituirne parte integrante e sostanziale (All.1-5), fatta salva ogni ulteriore modifica a seguito di verifica congiunta condotta con il referente incaricato da Lepida S.p.A.;
5. di dare atto che i dati di contatto del Responsabile della Protezione dei Dati Personali (RPD/DPO) saranno indicati nell'informativa redatta ai sensi dell'art. 13 del GDPR e pubblicati sul sito istituzionale dell'Azienda;
6. di approvare in via provvisoria, in attesa di implementare il lavoro con Lepida S.p.A., il registro del trattamento dei dati personali allegato al presente atto quale parte integrante e

sostanziale dello stesso (Allegato 6), dando atto che esso costituisce la prima base di lavoro su cui impostare l'attività con il referente di Lepida S.p.A.;

7. di rinviare a successivo atto l'approvazione del documento di valutazione dei rischi e della procedura prevista dall'art. 33 del GDPR, in caso di violazione dei dati con la conseguente notifica del *data breach*, ad esito del confronto con Lepida S.p.A. previsto dal relativo contratto di servizio;
8. di dare atto che, in attesa della formalizzazione della suddetta procedura, si individua in via provvisoria, nel Direttore o suo delegato, la figura incaricata di effettuare la segnalazione al Garante della Privacy, ai sensi dell'art. 33 del GDPR;
9. di dichiarare la presente deliberazione urgente e quindi immediatamente eseguibile;
10. di pubblicare la presente deliberazione all'Albo Pretorio on line dell'Azienda per la durata di 10 giorni consecutivi.

Letto, approvato e sottoscritto

Il Presidente



**PARERE DI REGOLARITA' TECNICA E CONTABILE**

Il Direttore esprime parere favorevole di regolarità tecnica e contabile del presente atto, ai sensi dell'art. 28 comma 6 dello Statuto aziendale.

Direttore



Delibera N.: 2018- 34

**La presente deliberazione è immediatamente eseguibile.**

Cla/Fasc. 1.5.4/2018

Reggio Emilia, li 25/05/2018