Allegato Tecnico Servizi di supporto per gli adempimenti GDPR

Nota di lettura

Lepida ScpA si riserva la facoltà di poter intervenire sulle misure tecniche e organizzative descritte nel presente documento, al fine di rendere il servizio conforme alle successive indicazioni normative che dovessero subentrare in argomento. Si riserva inoltre di intervenire per la correzione di meri errori materiali o refusi.

1. Descrizione del servizio

1.1 Definizione e Acronimi

- Community Network dell'Emilia-Romagna (CNER): con la Delibera DGR 758/2013 è stata approvata la Nuova convenzione per il funzionamento, la crescita e lo sviluppo della Community Network Emilia-Romagna (CNER) per creare le condizioni organizzative per dare attuazione alle finalità e ai progetti contenuti nel Piano Telematico dell'Emilia-Romagna, ora AdER Agenda Digitale dell'Emilia-Romagna, è

un'aggregazione territoriale su base regionale (Art. 30 TUEL), con propria sede (presso la sede della Regione Emilia-Romagna, cui è conferito potere di rappresentanza della CNER stessa), con una governance solida e partecipata, affidata al "Comitato Permanente di Indirizzo e Coordinamento con gli enti locali" (Art. 6, comma 4 LR 11/04), e con uno specifico ruolo attivo da parte della Società Lepida ScpA;

- Comitato Permanente di Indirizzo e Coordinamento (CPI): il Comitato Permanente di Indirizzo e Coordinamento con gli Enti locali, istituito con la Legge Regionale n.11/2004 e successive modifiche e integrazioni, è organismo della Community Network dell'Emilia-Romagna;
- Comitato Tecnico (CT): il Comitato Tecnico, istituito dalla Legge Regionale n. 11/2004 e successive modifiche e integrazioni , la cui composizione è disciplinata con apposita delibera della Giunta regionale, opera a supporto delle attività del CPI;
- ADER: Agenda Digitale dell'Emilia-Romagna;
- Comunità Tematiche: strumento messo a disposizione di tutta la Pubblica Amministrazione locale dell'Emilia-Romagna come azione strategica di ADER per la realizzazione dell'amministrazione digitale e aperta come prevista dalla Legge 124/2015 di riforma della Pubblica Amministrazione.
- GDPR: Regolamento Europeo 2016/679/UE per la protezione dei dati personali.

1.2 Descrizione generale

Lepida ScpA fornisce agli Enti Soci i seguenti servizi di supporto per gli adempimenti e adeguamenti derivanti dal Regolamento Europeo 2016/679/UE per la protezione dei dati personali (GDPR):

- 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;
- funzione di Responsabile della protezione dati (RPD, ovvero DPO);
- strumento per il registro dei trattamenti (RecordER).

La sostenibilità dei servizi di Lepida ScpA è basata su un modello partecipato dagli Enti nell'ambito delle Comunità Tematiche per la definizione e condivisione dei procedimenti, delle tipologie di dati e dei relativi trattamenti nell'ottica di omogeneizzazione delle modalità di trattamento a livello regionale.

L'erogazione dei servizi da parte di Lepida ScpA prevede una chiara suddivisione dei compiti e delle responsabilità tra l'Ente e Lepida ScpA. Gli adempimenti del GDPR sono di responsabilità dell'Ente e coinvolgono l'intera struttura organizzativa e i processi gestionali

interni, oltre agli aspetti tecnici. I servizi di Lepida ScpA sono quindi un supporto importante, ma non sostitutivi dei compiti e degli impegni dell'Ente. Infatti, si precisa che la responsabilità della conformità al regolamento GDPR rimane in capo al titolare del trattamento, ovvero colui che determina le finalità e i mezzi del trattamento di dati personali.

Si sottolinea altresì che la responsabilità del censimento e strutturazione dei processi interni rimane in capo all'Ente così come la responsabilità del popolamento ed aggiornamento costante del Registro dei trattamenti. L'Ente, anche in qualità di titolare del trattamento, si obbliga a fornire a Lepida ScpA tutte le informazioni complete e a garantire le condizioni per l'espletamento dei servizi.

Si precisa altresì che il ruolo di DPO è incompatibile con il responsabile dei sistemi informativi dell'Ente; è incompatibile con il responsabile dell'anticorruzione e trasparenza (su indicazione del garante) e che il DPO non svolge compiti e funzioni di responsabile della transizione digitale previsto dal CAD.

I servizi di Lepida ScpA prevedono due componenti principali:

- **setup iniziale**: Lepida ScpA effettua una analisi e valutazione della situazione esistente sulla base delle informazioni fornite dall'Ente ed elabora un piano di azione per la conformità dei trattamenti al GDPR.
- **supporto e Responsabile della protezione dati (DPO)**: Lepida ScpA fornisce il servizio di supporto alla gestione e mantenimento della conformità e di Responsabile della protezione dati (DPO) nell'ambito di un modello organizzativo che l'Ente dovrà adottare per l'inclusione della funzione del DPO nei propri processi.

Lepida ScpA fornisce inoltre un servizio cloud di registro dei trattamenti (RecordER) realizzato sulla base di specifiche funzionali definite insieme agli Enti, nell'ambito delle attività delle Comunità Tematiche, a supporto degli Enti e di Lepida ScpA per la gestione del registro dei trattamenti e tutte le informazioni collegate.

Per l'erogazione dei servizi Lepida ScpA si avvale di supporto legale e tecnico adeguato, opportunamente selezionato.

1.4 Descrizione dei servizi offerti

I servizi offerti da Lepida ScpA vengono di seguito descritti.

Si sottolinea che le attività e i servizi di Lepida ScpA si basano su un modello di trattamenti/procedimenti definito nell'ambito delle attività delle Comunità Tematiche e sull'utilizzo di uno strumento per il registro dei trattamenti (RecordER). La sostenibilità dei servizi di Lepida ScpA è basata quindi sulla omogeneizzazione dei trattamenti e standardizzazione dei processi nell'ambito delle attività delle Comunità Tematiche e dello specifico Gruppo di Lavoro ivi previsto.

1.4.1. Servizio di setup iniziale

Il servizio riguarda principalmente l'analisi e valutazione della situazione esistente che mira ad individuare i trattamenti da sottoporre a valutazione. Al fine di effettuare la valutazione è indispensabile per Lepida ScpA acquisire tutte le informazioni, i dati e la documentazione complete, sotto la responsabilità dell'Ente. Saranno organizzati incontri mirati con l'Ente per approfondire tutte le informazioni fornite e i dettagli attinenti il censimento dei dati, dei trattamenti effettuati sui dati personali, sui processi e politiche in uso, sui ruoli e responsabilità, sui sistemi, applicazioni e basi dati.

Lepida ScpA svolge l'analisi e la valutazione delle informazioni fornite dall'Ente e raccolte attraverso gli incontri ed in particolare vengono svolte: analisi dei dati personali; analisi dei trattamenti, valutazione delle contromisure organizzative e procedurali esistenti; valutazione delle contromisure tecnologiche esistenti. Quindi Lepida ScpA procede all'elaborazione del piano di azione contenente le contromisure necessarie per essere conformi ai requisiti del GDPR. Il piano comprende: le contromisure organizzative e di processo proposte per la conformità, le contromisure tecnologiche proposte per la conformità, le revisioni e integrazioni necessarie dei documenti (informative, clausole contrattuali, sicurezza, ..) e le priorità di intervento.

1.4.2. Servizio di funzioni DPO

Il servizio riguarda principalmente il ruolo di Responsabile della protezione dati (DPO) e il supporto alla gestione e mantenimento della conformità al GDPR , ovvero, all'aggiornamento dei processi, delle procedure, e delle funzioni necessarie per il rispetto del GDPR.

Il GDPR prevede l'obbligo per gli Enti pubblici di designare il DPO con compiti, funzioni e ruolo all'interno dell'Ente. L'inclusione del DPO nei processi dell'Ente dovrà essere disciplinata in maniera peculiare nel modello organizzativo che l'Ente dovrà adottare per la gestione degli adempimenti alla normativa.

Pertanto, i servizi di Lepida ScpA riguardano principalmente, e in stretta aderenza a quanto predisposto dal GDPR, le attività di informazione e consulenza in ordine agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, sorveglianza dell'applicazione della normativa in materia di protezione dei dati e delle policy adottate

dall'Ente in materia, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo, fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento, cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

1.4.3. Servizio cloud RecordER

Lepida ScpA ha definito insieme agli Enti, nell'ambito delle Comunità tematiche, le specifiche funzionali di uno strumento telematico coerente con il modello dei procedimenti trattamenti individuato e ha realizzato il servizio cloud RecordER per la gestione del registro dei trattamenti e tutte le informazioni collegate.

Il servizio permette di strutturare le informazioni storicizzate relative ai trattamenti ai dati includendo:

- organigramma dell'Ente, unità organizzative e personale;
- procedimenti, trattamenti, ambiti e relativi collegamenti;
- categorie dei dati e degli interessati dei trattamenti e termini di cancellazione;
- ruoli, responsabilità e misure di sicurezza;
- gestione di fornitori e soggetti esterni;
- mappatura delle soluzioni software utilizzate dagli Enti.

Il servizio, che permette numerose funzionalità utili per condividere informazioni, potrà avere continue evoluzioni ed arricchimenti coerenti con i risultati dei lavori delle Comunità Tematiche. Il servizio permette a ciascun Ente una gestione autonoma delle proprie informazioni in relazione a procedimenti e trattamenti regionali di riferimento. Sono previste funzionalità di import ed export per facilitare il popolamento iniziale e l'aggiornamento di alcune delle informazioni base dell'Ente.

1.4.4. Servizio di formazione

Le attività e i servizi dei Lepida ScpA includono anche la formazione per i vertici degli Enti e che viene arricchita, in collaborazione con la Regione Emilia-Romagna, con materiali informativi e formativi a beneficio di tutto il personale dell'Ente con percorsi formativi on line sfruttando le piattaforme e le infrastrutture telematiche regionali previsti da ADER.

2. Attivazione dei servizi

L'attivazione dei servizi di supporto per gli adempimenti GDPR richiede la nomina da parte dell'Ente, e la comunicazione a Lepida ScpA, di un proprio referente incaricato di ricevere ed inviare le comunicazioni, le versioni preliminari delle relazioni prodotte da Lepida ScpA ed

operare in qualità di coordinatore delle attività nei confronti dei soggetti interni coinvolti. L'Ente si impegna a comunicare il proprio referente al momento dell'adesione al servizio e a comunicare tempestivamente a Lepida ScpA eventuale variazione del referente.

Il referente nominato dall'Ente dovrà garantire la disponibilità delle informazioni, della documentazione e dei soggetti interni per condurre le attività di analisi e valutazione, nonché gli incontri mirati di approfondimento. L'Ente dovrà garantire a Lepida ScpA l'accesso a tutta la documentazione, tutte le informazioni e ai sistemi rilevanti ai fini dello svolgimento dei servizi.

Lepida ScpA dovrà essere designata responsabile del trattamento.

2.1 Processo di attivazione

L'Ente deve comunicare a Lepida ScpA le informazioni complete necessarie per l'attivazione dei servizi secondo le procedure e le modalità di trasmissione previste da Lepida ScpA.

Le informazioni riguardano principalmente:

- tutti i dati dell'Ente, i dati del referente (nome, cognome, e-mail, telefono);
- tutta la documentazione disponibile, che a titolo indicativo e non esaustivo includono:
    - Organigramma e declaratorie strutture;
    - Modello organizzativo privacy;
    - DPS (Documento Programmatico sulla Sicurezza);
    - Atto designazioni incaricati;
    - Elenco amministratori di sistema;
    - Atti designazione individuale Amministratori di Sistema (AdS);
    - Censimento trattamenti (se non presente in DPS);
    - Censimento processi;
    - Designazioni responsabili esterni e verifiche sugli stessi;
    - Policy incidenti sicurezza;
    - Policy Business Continuity;
    - Business Impact Analysis;
    - Elenco interventi formativi in materia di privacy;
    - Regolamento utenti utilizzo strumenti;
    - Policy amministratori di sistema;
    - Policy verifiche di sicurezza e controlli su utenti e applicazioni;
    - Policy videosorveglianza;
    - Policy gestione accessi sedi Ente;

- Convenzioni fruibilità dati;
- Regolamento dati sensibili e giudiziari;
- Verbali ispezioni/sanzioni Garante;
- Eventuali certificazioni ISO;
- Altri documenti utili.

Tutte le comunicazioni relative al servizi e alle modalità di attivazione devono essere inviate all'indirizzo email: gdpr@lepida.it .

L'Ente deve inoltre assicurare il popolamento ed il costante aggiornamento, a proprio carico, delle informazioni e dei dati nel sistema RecordER.

L'attivazione del servizio, da parte di Lepida ScpA, avviene attraverso la nomina di un referente per l'Ente e alla ricezione delle informazioni richieste.

3. Erogazione del servizio

3.1 Fase di setup iniziale

Lepida ScpA procede con le attività di analisi delle informazioni raccolte e all'organizzazione di incontri per approfondire i dettagli attinenti il censimento dei dati, dei trattamenti effettuati sui dati personali, sui processi e politiche in uso, sui ruoli e responsabilità, sui sistemi, applicazioni e basi dati.
Lepida ScpA elabora una prima relazione contenente la descrizione del materiale e delle informazioni raccolte (**Milestone 1**).

Lepida ScpA provvede all'analisi e alla valutazione delle informazioni fornite dall'Ente e raccolte attraverso gli incontri, prevedendo, ove è necessario, ulteriori incontri confronto con l'Ente e in particolare con il responsabile dei sistemi informativi relativamente alle tecnologie e ai servizi ICT utilizzati dagli Enti.
Lepida ScpA elabora una seconda relazione sugli esiti delle valutazioni con i rischi, le criticità e le non conformità rilevate in relazione agli aspetti organizzativi, procedurali e tecnologici (**Milestone 2**).

Lepida ScpA procede quindi all'elaborazione del piano di azione contenente le contromisure necessarie per essere conformi ai requisiti del GDPR. Il piano comprende: le contromisure organizzative e di processo proposte per la conformità; le contromisure tecnologiche

proposte per la conformità; le revisioni e integrazioni necessarie dei documenti (informative, clausole contrattuali, sicurezza, ..) e le priorità di intervento (**Milestone 3**).

Il piano viene consegnato all'Ente con una presentazione dei risultati e si conclude di fatto la fase iniziale del servizio di Lepida ScpA.

3.1.1 Tempistica

Le tempistiche di realizzazione di tale fase dipendono inevitabilmente dalla dimensione dei processi dell'Ente, dal grado di conformità alla normativa in materia di privacy e sicurezza e dal quantità e qualità delle informazioni e della documentazione raccolta. Il completamento delle attività può comunque essere stimato nel termine di 90 giorni.

3.2 Fase di gestione e DPO

3.2.1 Modalità di erogazione

Lepida ScpA definisce e concorda con l'Ente un flusso informativo costante ed incessante, anche in contradditorio, al fine di valutare gli impatti della normativa attuale e di futura cogenza. Fornisce, inoltre, supporto all'organizzazione nella definizione delle policy in materia di protezione dei dati e sicurezza delle informazioni, esprimendo formale parere obbligatorio.

Lepida ScpA propone modulistica (fra cui designazione dei responsabili del trattamento, informative e consensi) in aderenza alla normativa. Partecipa alla progettazione di nuove applicazioni o alla modifica sostanziale di quelle esistenti in aderenza al principio della privacy by design. Fornisce supporto nella definizione delle misure più idonee ed efficaci a garantire l'esercizio dei diritti degli interessati e formula gli indirizzi per il popolamento e l'aggiornamento del Registro delle attività di trattamento (RecordER).

Lepida ScpA fornisce parere preventivo obbligatorio in ordine all'adozione delle misure più adeguate ed efficaci 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.

Lepida ScpA fornisce indicazioni in ordine alla metodologia da adottare ai fini della valutazione d'impatto e assiste l'Ente nell'espletamento della stessa.

Lepida ScpA garantisce la propria assistenza in caso di visite ispettive dell'Autorità Garante (o delle forze dell'ordine) o di interazione con la medesima Autorità per qualsiasi questione connessa ai trattamenti di dati personali effettuati dall'organizzazione. Fornisce inoltre supporto e coopera con la struttura competente nei casi di incidenti di sicurezza.

Lepida ScpA svolge una formazione annuale per il personale dell'Ente oltre alla messa a disposizione del materiale formativo realizzato in collaborazione con Regione Emilia-Romagna reso disponibile sulle piattaforme regionali.

Lepida ScpA svolge specifici audit, a partire dal secondo anno, le cui modalità saranno svolte in accordo con l'Ente.

3.2.2 Modalità espressione dei pareri DPO

Lepida ScpA esprime il proprio parere, nella funzione di DPO, in tutti i casi richiesti dalla normativa e dal modello organizzativo definito dall'Ente, utilizzando modalità e strumenti che sono concordati con l'Ente e che ne assicurino la certezza della trasmissione.

3.2.3 Help Desk

La segnalazione di eventuali richiesta attinenti i servizi deve avvenire attraverso il servizio di Help Desk disponibile dal **lunedì al venerdì dalle ore 8:30 alle ore 18:30 ed il sabato dalle ore 8.30 alle ore 13.30**. I riferimenti dell'Help Desk sono:

Telefono	**800 445500**
e-mail	helpdesk@lepida.it
Web	https://www.lepida.net/assistenza