lepida

Allegato Tecnico

Servizi di supporto per
gli adempimenti GDPR

Nota di lettura 4
1. Descrizione del Servizio 4
1.1. Definizioni e acronimi 4
1.2. Descrizione generale 5
1.3. Descrizione dei servizi offerti 7
1.3.1. Servizio di setup iniziale 7
1.3.2. Servizi di funzione RPD ovvero DPO 7
1.3.3. Servizio cloud RecordER 8
1.3.4. Servizi di formazione 9
1.3.5. Servizi di Data Protection Room 9
2. Attivazione dei servizi 9
2.1. Processo di attivazione 9
3. Erogazione del servizio 11
3.1. Fase di setup iniziale 11
3.1.1. Tempistica 11
3.2. Fase di gestione e RPD 11
3.2.1. Modalità di erogazione 11
3.2.2. Modalità espressione dei pareri RPD 12
4. Servizio di assistenza 12
5. Esercizio del servizio RecordER 13
5.1. Disponibilità del servizio 13
5.2. Assistenza in esercizio 14
5.2.1. Help Desk 14
5.2.2. Manutenzione correttiva 14
5.3. Livelli di servizio (SLA) 14

release	200
data	05.09.2023
redazione documento	Alfredina Di Felice - Mary Porcaro - Riccardo Bevilacqua
verifica documento	Sergio Duretti - Anna Lisa Minghetti - Giuseppe Sberlati - Lorenzo Fabbricatore
approvazione documento	Gianluca Mazzini

Nota di lettura

LepidaScpA, di seguito Lepida, si riserva la facoltà di poter intervenire sulle misure tecniche e organizzative descritte nel presente documento, al fine di rendere il sistema 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. Definizioni 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.

- **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.

- **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.
- **Data Protection Officer (DPO) o Responsabile per la Protezione dei Dati (RPD)** - è una figura introdotta dal Regolamento generale per la protezione dei dati personali (GDPR), Capo IV Sezione 4, Artt. 37, 38 e 39. Sono tenuti alla sua designazione il titolare e il responsabile del trattamento, nei casi previsti dall'art. 37, par. 1, lett. a), b) e c). Il RPD è designato in funzione delle sue qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti di cui all'articolo 39 GDPR: informazione, formazione, consulenza e sorveglianza dell'adempimento della disciplina privacy. Il suo nominativo deve essere comunicato al Garante, in quanto coopera e costituisce il punto di contatto con l'Autorità per le questioni connesse al trattamento dei dati personali.

1.2. Descrizione generale

Lepida 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 (in breve 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;
- Attività di definizione congiunta, tramite tavoli di lavoro chiamati "Data Protection Room", di policy, linee guida generali, prassi operative, template e modelli a disposizione degli Enti;
- Attività di formazione generale e avanzata tramite webinar;
- Attività di sorveglianza generale sull'applicazione del Regolamento Europeo 2016/679;
- Funzione di Responsabile della Protezione Dati (RPD) ovvero DPO (Data Protection Officer);
- Strumento per il registro dei trattamenti (RecordER).

L'erogazione dei servizi da parte di Lepida prevede una chiara suddivisione dei compiti e delle responsabilità tra l'Ente e Lepida. 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 sono quindi un supporto importante, ma non possono essere 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 e aggiornamento costante del Registro dei trattamenti. L'Ente, anche in qualità di titolare del trattamento, si obbliga a fornire a Lepida tutte le informazioni complete e a garantire le condizioni per l'espletamento dei servizi.

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

I servizi di Lepida si articolano in:

- Setup iniziale per gli Enti che si avvalgono per la prima volta del servizio di Lepida, consistente nello svolgimento di una analisi e valutazione della situazione esistente sulla base delle informazioni fornite dall'Ente a cui si fa seguire la condivisione di un piano generale di azione per la conformità dei trattamenti al GDPR;

- Attività di consulenza e sorveglianza come previste dal Regolamento Europeo al fine di assolvere al ruolo di Responsabile della Protezione dei Dati (RPD): Lepida fornisce supporto alla gestione e mantenimento della conformità al Regolamento Europeo 679/2016 e di Responsabile della Protezione Dati (RPD) nell'ambito del modello organizzativo in materia di protezione dei dati personali adottato dall'Ente. Lepida fornisce inoltre uno strumento in cloud per la gestione

del registro dei trattamenti - RecordER - realizzato sulla base di specifiche funzionali definite insieme agli Enti.

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

1.3. Descrizione dei servizi offerti

I servizi offerti da Lepida vengono di seguito descritti.

Si sottolinea che le attività e i servizi di Lepida si basano su un modello di trattamenti/procedimenti a suo tempo 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 è basata quindi sulla omogeneizzazione dei trattamenti e standardizzazione dei processi.

1.3.1. Servizio di setup iniziale

Il servizio rivolto agli Enti che si avvalgono per la prima volta del servizio di Lepida 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 acquisire tutte le informazioni, i dati e la documentazione complete predisposte dall'Ente dall'entrata in vigore del Regolamento Europeo 679/2016. 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.

Alla luce dell'analisi condotta l'Ente e Lepida predispongono un piano generale di azione contenente le misure necessarie per la conformità ai requisiti del GDPR.

1.3.2. Servizi di funzione RPD ovvero DPO

Il servizio riguarda il ruolo di Responsabile della Protezione dei Dati (RPD ovvero DPO) secondo quanto previsto dal Regolamento Europeo 679/2016 con particolare attenzione ai compiti ivi indicati di consulenza e sorveglianza sull'applicazione del Regolamento.

Il GDPR prevede l'obbligo per gli Enti pubblici di designare il RPD con compiti, funzioni e ruolo all'interno dell'Ente. L'inclusione del RPD nei processi dell'Ente deve essere disciplinata nel modello organizzativo in materia di protezione dei dati personali adottato dall'Ente. Pertanto, i servizi di Lepida riguardano principalmente, e in stretta aderenza a quanto previsto dal GDPR, le attività di informazione e consulenza in ordine agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, la 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, nonché la fornitura, se richiesto, di un parere in merito alla valutazione d'impatto sulla protezione dei dati, la cooperazione con l'Autorità di controllo e lo svolgimento della funzione di punto di contatto per l'Autorità di controllo per questioni connesse al trattamento..

1.3.3. Servizio cloud RecordER

Lepida ha definito insieme agli Enti le specifiche funzionali di uno strumento digitale coerente con il modello dei procedimenti individuati a suo tempo nel Gruppo di Lavoro delle Comunità Tematiche e ha realizzato RecordER, servizio in cloud per la gestione del registro dei trattamenti e tutte le informazioni collegate.

RecordER permette di strutturare le informazioni storicizzate relative ai trattamenti dei 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
- Gestione degli incidenti di sicurezza
- Storicità delle informazioni

Lo strumento permette a ciascun Ente una gestione autonoma delle proprie informazioni in relazione a procedimenti e trattamenti di riferimento. Sono previste

funzionalità di import ed export per facilitare il popolamento iniziale e l'aggiornamento di alcune delle informazioni base dell'Ente.

1.3.4. Servizi di formazione

Le attività e i servizi di Lepida includono la formazione generale e avanzata per i vertici degli Enti e che può essere arricchita, anche in collaborazione con la Regione Emilia-Romagna, con l'organizzazione di specifici webinar comprensivi di materiali informativi e formativi a beneficio di tutto il personale dell'Ente sfruttando le piattaforme e le infrastrutture telematiche regionali in essere oppure messe a disposizione da Lepida stessa.

1.3.5. Servizi di Data Protection Room

Ai servizi previsti dal Regolamento si aggiungono dal 2023 i servizi sopra descritti di Data Protection Room, ovvero di definizione congiunta con gli Enti di di policy, linee guida generali, prassi operative, template e modelli a disposizione degli Enti.

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, di un proprio referente incaricato di ricevere e inviare le comunicazioni che agisca 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 l'eventuale variazione del referente.

Il referente dell'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 l'accesso a tutta la documentazione, a tutte le informazioni e ai sistemi rilevanti ai fini dello svolgimento dei servizi.

Per tali attività Lepida dovrà essere designata responsabile del trattamento.

2.1. Processo di attivazione

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

Le informazioni riguardano principalmente:

- Tutti i dati dell'Ente, i dati del referente (nome, cognome, email, 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 e il costante aggiornamento, a proprio carico, delle informazioni e dei dati nel sistema RecordER.

L'attivazione del servizio, da parte di Lepida, 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 procede con le attività di analisi delle informazioni ricevute dall'Ente che ha aderito al servizio 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.

L'Ente e Lepida procedono all'elaborazione di un piano generale di azione contenente le misure necessarie per essere conformi ai requisiti del GDPR.

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 dalla quantità e qualità delle informazioni e della documentazione raccolta. Il completamento delle attività può comunque essere stimato nel termine di 60 giorni.

3.2. Fase di gestione e RPD

3.2.1. Modalità di erogazione

Lepida definisce e concorda con l'Ente un flusso informativo costante, anche in contraddittorio, 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 formali pareri.

Lepida 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 fornisce indicazioni in ordine alla metodologia da adottare ai fini della valutazione d'impatto ed eventualmente fornisce all'Ente un parere finale.

Lepida costituisce su temi di comune interesse degli Enti, gruppi di lavoro (denominati "Data Protection Room") a cui partecipino referenti degli Enti interessati con l'obiettivo di definire insieme su uno specifico tema policy, linee guida, template comuni, congiuntamente con il team di esperti di Lepida.

Lepida 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 organizza ogni anno attività di formazione in forma di webinar per il personale dell'Ente oltre alla messa a disposizione del materiale realizzato.

Lepida può svolgere specifici audit secondo modalità concordate con l'Ente.

3.2.2. Modalità espressione dei pareri RPD

Lepida esprime pareri tramite la funzione di RPD, in tutti i casi richiesti dalla normativa e dal modello organizzativo definito dall'Ente, utilizzando modalità e strumenti che sono concordati con l'Ente.

Lepida prende in carico la richiesta di parere entro massimo 2 giorni lavorativi, mentre la tempistica per la formulazione del parere è soggetta alla complessità della richiesta nonché agli approfondimenti e alle interlocuzioni che si rendano necessarie.

4. Servizio di assistenza

La segnalazione di eventuali richieste attinenti i servizi deve avvenire con le seguenti modalità:

- richieste di informazioni relative al Regolamento UE 2016/679 e di informazioni e/o assistenza tecnico/operativa sull'utilizzo della piattaforma RecordER: gdpr@lepida.it;
- richieste di pareri inerenti la funzione di RPD/DPO: dpo-team@lepida.it;
- segnalazioni di eventuali data breach: dpo-team@lepida.it oltre ad esplicito contatto telefonico al proprio referente.

La segnalazione di problemi sul servizio RecordER deve invece avvenire attraverso il servizio di Assistenza come di seguito indicato.

5. Esercizio del servizio RecordER

5.1. Disponibilità del servizio

Il servizio è disponibile all'utenza H24 ad eccezione delle finestre temporali necessarie per eventuali interventi di manutenzione ordinaria e straordinaria.

Lepida ScpA procede ad effettuare operazioni di manutenzione programmata, anche durante le ore di normale apertura degli uffici. Rientrano nelle attività di manutenzione programmata tutti gli aggiornamenti correttivi, funzionali e di sistema. Nel caso in cui la manutenzione programmata richieda l'indisponibilità del servizio, questa sarà preventivamente notificata per email agli Enti. Nella email verranno forniti gli estremi temporali presunti del fermo, non vincolanti per Lepida ScpA.

Lepida ScpA garantisce i seguenti livelli di servizio (SLA) per la manutenzione programmata:

Parametro	**Valore**	**SLA (su base quadrimestrale)**
Tempo minimo di avviso in caso di disservizio per manutenzione programmata di competenza Lepida ScpA	3 giorni solari	90% dei casi

5.2. Assistenza in esercizio

Lepida ScpA fornisce due tipi di assistenza in esercizio:

- Servizio di help desk
- Manutenzione correttiva

5.2.1. Help Desk

La segnalazione di eventuali malfunzionamenti e la richiesta di assistenza tecnica devono 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

Lepida ScpA non garantisce alcun livello di servizio per le segnalazioni inoltrate tramite canali diversi dall'Help Desk.

5.2.2. Manutenzione correttiva

Per manutenzione correttiva si intendono gli interventi di correzione di malfunzionamenti del sistema che non possono essere risolti attraverso semplici operazioni di configurazione, ma necessitano di operazioni di modifica software oppure aggiornamento di una o più componenti del sistema, purché inerenti funzionalità già previste dal sistema.

5.3. Livelli di servizio (SLA)

I valori di SLA, su base quadrimestrale, riportati di seguito si riferiscono alla finestra temporale di disponibilità del servizio di Help Desk ed esclusivamente alle attività di competenza di Lepida ScpA relativamente al servizio RecordER:

Tempo di diagnosi in caso di malfunzionamento bloccante	240 minuti	85% dei casi
Tempo di diagnosi in caso di malfunzionamento non bloccante	480 minuti	85% dei casi
Tempo di risoluzione, anche provvisoria di malfunzionamenti bloccanti che non richiedono manutenzione correttiva	480 minuti	75% dei casi
Tempo di risoluzione, anche provvisoria di malfunzionamenti non bloccanti che non richiedono manutenzione correttiva	960 minuti	75% dei casi