

LepidaID

Relazione trattamento dati personali



1. Introduzione	3
1.1. Storia del documento	3
2. Privacy e trattamento dei dati personali	4
3. Informazioni trattate	6
3.1. Verifiche tramite ANPR e SCIPAFI e principio di minimizzazione	6
3.2. Identità Digitale ad uso privato o ad uso professionale per persona fisica	7
3.2.1. Persone fisiche	7
3.3. Identità Digitale ad uso professionale per persona giuridica	7
3.3.1. Persona giuridica ad uso professionale	8
3.4. Identificazione dell'utente	8
3.4.1. Identificazione a mezzo webcam con operatore	11
3.4.2. Identificazione a mezzo videoregistrazione e bonifico bancario	11
3.5. Amministrazione del sistema	12
3.6. Gestione dei documenti e dei log	12
3.7. Sicurezza	14
4. Informativa agli utenti	16

1. Introduzione

La presente relazione mira a descrivere i trattamenti di dati personali effettuati da Lepida ScpA, di seguito Lepida, nell'ambito del servizio LepidaID riportandone le informazioni essenziali e le misure messe in atto per conformare tali trattamenti alla normativa sulla protezione dei dati personali.

1.1. Storia del documento

Versione	Data	Cambiamenti apportati
1.0	28/11/2017	Prima stesura
1.1	16/02/2018	Seconda stesura
1.2	15/05/2018	Versione Aggiornata - Modificato paragrafo 3.1 "Richiesta identità digitale": distinzione esplicita tra attributi obbligatori e opzionali - Modificato il paragrafo 4 "Informativa agli utenti": modificato "Periodo di conservazione dei dati" - Modificato paragrafo 3.4 Gestione dei documenti e dei log con aggiunta del dettaglio in merito alle modalità di conservazione dei log
1.3	15/06/2018	Versione Aggiornata Modificato paragrafo 3.1 "Richiesta identità digitale"
1.4	17/03/2020	Versione Aggiornata - Aggiunto paragrafo "3.2.1 Identificazione a mezzo webcam" - Aggiornamenti minori - Aggiornata l'informativa sul trattamento dei dati personali per gli utenti
1.5	01/10/2020	Versione Aggiornata - Aggiunto "domicilio fisico" come Attributo secondario. - Aggiunto paragrafo "3.2.2 Identificazione a mezzo videoregistrazione e bonifico bancario" - Aggiornamenti minori
1.6	30/12/2021	Versione Aggiornata Aggiunto paragrafo "3.2 Identità digitale ad uso professionale per persona giuridica"

		• Aggiornamenti minori
1.7	22/06/2022	Versione Aggiornata • Aggiunta riconoscimento attraverso CIE 3.0 • Eliminati capitoli sulla gestione dei cookies in quanto gestiti su una informativa a parte (sito id.lepida.it) • Aggiornamenti minori
1.8	23/08/2022	Versione Aggiornata • Aggiornamento logo Lepida ScpA, stile e impaginato
1.9	06/12/2022	Versione Aggiornata • Introduzione SPID LepidaID per minori • Aggiunta la possibilità di ottenere identità digitale SPID LepidaID anche per soggetti con documenti di identità emessi dalla Repubblica di San Marino
2.0	20.04.2023	Versione Aggiornata • Aggiornamenti
2.1	26.06.2024	Versione Aggiornata • Integrato art. 7 dell'Informativa agli utenti
2.2	21.04.2026	Versione Aggiornata • Aggiornato logo • Aggiornati par. 4.6 e 4.9 per introduzione possibilità per l'utente di trasmettere la richiesta di non attivazione dell'identità digitale SPID • Aggiornato il paragrafo 4 "Informativa agli utenti": modificato "Periodo di conservazione"
2.3	26.08.2026	Versione Aggiornata • Aggiornati par. 3, 6, 7 a valle dell'adeguamento ai controlli ANPR

2. Privacy e trattamento dei dati personali

Preliminarmente, deve essere rappresentato che la scelta di accreditamento di Lepida come IDP SPID nacque dalla volontà della Regione Emilia-Romagna e dalla comunità degli Enti pubblici, cosiddetta Community Network dell'Emilia-Romagna CNER, prevista dalla Legge Regionale 11/2004 "Sviluppo regionale della Società dell'informazione", di valorizzare l'esperienza pluriennale e l'identità pregressa del sistema di autenticazione



denominato FedERa (Federazione degli Enti dell'Emilia-Romagna per l'Autenticazione). Tale sistema fu realizzato da Regione Emilia-Romagna, attraverso Lepida, nell'ambito della CNER, al fine di permettere ai cittadini di acquisire identità digitali (credenziali) con le quali poter richiedere l'accesso ai servizi online erogati dai diversi soggetti aderenti al sistema (Regione, Enti Locali, altre PP.AA. e soggetti di natura pubblica o privata), mediante un sistema di autenticazione federata.

L'ottica del riutilizzo delle identità pregresse di FedERa e le funzioni di Identity Provider SPID, svolte da Lepida su mandato dei soci, posero la stessa società in condizioni di contitolarità dei trattamenti di dati personali afferenti a tale servizio, ai sensi e per gli effetti di cui all'art. 26 del Regolamento UE n. 679/2016.

Rinviando all'esauriente relazione sull'argomento del documento "Modello organizzativo SPID e utilizzo dei dati", in tale sede si rappresenta che gli Enti soci e Lepida hanno disciplinato la contitolarità in uno specifico accordo ex art. 26 del Regolamento UE 2016/679, in cui hanno regolamentato il corretto inquadramento teorico dei rispettivi ruoli (a titolo esemplificativo, l'accordo prevederebbe la responsabilità di Lepida in caso di data breach, sia con riferimento alla notifica all'Autorità Garante sia con l'esaudimento delle comunicazioni di cui all'art. 34 del Regolamento).

Per quel che concerne, invece, l'assolvimento dell'onere informativo nei confronti degli utenti FedERA, i due soggetti contitolari effettuano un trattamento di dati personali per finalità diverse da quelle per le quali i dati sono stati inizialmente raccolti. Tale facoltà è consentita dal nuovo regolamento europeo solo se il nuovo trattamento risulti essere compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. Vien da sé che il servizio che gli Enti Soci e Lepida, agendo come IdP di SPID, forniscono, è evidentemente sovrapponibile a quello originario per cui i dati furono raccolti (FedERa).

Si precisa che il perimetro della suddetta contitolarità è limitato alle sole identità pregresse promananti dal sistema di autenticazione denominato FedERa (Federazione degli Enti dell'Emilia-Romagna per l'Autenticazione). D'altra parte, per i trattamenti di dati personali effettuati per le finalità di attribuzione dell'identità digitale e di fruizione dei servizi erogati online dai "Fornitori di servizi" tramite il Sistema Pubblico per la gestione dell'Identità Digitale (SPID), Lepida agisce in qualità di autonomo titolare.

3. Informazioni trattate

Nel rispetto delle linee guida AgID viene effettuata, in caso di creazione di nuova identità digitale, una chiara distinzione tra i dati anagrafici richiesti all'utente strettamente necessari per l'ottenimento dell'identità digitale e le informazioni aggiuntive non obbligatorie raccolte a discrezione del gestore a fini commerciali.

Lepida si limita, come IDP SPID, a richiedere e a trattare esclusivamente i dati strettamente necessari per l'ottenimento dell'identità digitale e non richiede informazioni aggiuntive né utilizza i dati raccolti per finalità ulteriori.

Tali informazioni possono essere trattate soltanto da soggetti all'uopo designati incaricati per il trattamento dei dati personali effettuato a mezzo del sistema informativo IdM (Identity Management) realizzato e gestito da Lepida.

Tutte le operazioni vengono svolte in conformità ai principi generali di cui all'art. 5 del Regolamento UE 2016/679 nel pieno rispetto delle normative e delle Linee Guida AgID relative a SPID.

3.1. Verifiche tramite ANPR e SCIPAFI e principio di minimizzazione

Nell'ambito delle procedure di rilascio, attivazione e gestione delle identità digitali SPID LepidaID, Lepida effettua verifiche automatiche e sincrone mediante l'interconnessione con l'Anagrafe Nazionale della Popolazione Residente (ANPR) e il sistema pubblico di prevenzione delle frodi SCIPAFI.

In ottemperanza al principio di minimizzazione del GDPR (Art. 5, par. 1, lett. c), i dati personali e gli attributi anagrafici recuperati attraverso i servizi di ANPR rappresentano rigorosamente il set minimo di informazioni strettamente necessarie alla realizzazione dei controlli di coerenza dei dati forniti dall'utente e alla verifica dell'esistenza in vita dello stesso. Tali informazioni non vengono in alcun modo eccedute o memorizzate per finalità diverse da quelle strettamente correlate alla validazione dell'identità e alla sicurezza del sistema.



3.2. Identità Digitale ad uso privato o ad uso professionale per persona fisica

Vengono richiesti e trattati i dati essenziali per l'erogazione del servizio che comprendono i dati di seguito riportati e una memorizzazione di una copia per immagini, ovvero scannerizzazione, fronte/retro di un documento di identità e della tessera sanitaria.

3.2.1. Persone fisiche

Vengono richiesti e trattati i seguenti dati:

Attributi Identificativi

- Nome
- Cognome
- Luogo di nascita
- Data di nascita
- Sesso
- Codice fiscale
- Nazione di nascita
- Provincia di nascita
- Estremi del documento di identità
- Indirizzo di posta elettronica

Attributi secondari

- Telefono mobile
- PEC (opzionale)
- Domicilio fisico.

3.3. Identità Digitale ad uso professionale per persona giuridica



Vengono richiesti e trattati i dati essenziali per l'erogazione del servizio che comprendono i dati di seguito riportati e una memorizzazione di una copia per immagini, ovvero scannerizzazione, fronte/retro di un documento di identità e della tessera sanitaria.

3.3.1. Persona giuridica ad uso professionale

Vengono richiesti e trattati i seguenti dati:

Attributi identificativi

- Password
- Cognome e nome (persona fisica)
- Sesso (persona fisica)
- Data di nascita (persona fisica)
- Nazione di nascita (persona fisica)
- Provincia di nascita (persona fisica)
- Luogo di nascita (persona fisica)
- Codice fiscale (persona fisica);
- Estremi di un valido documento di identità (persona fisica)
- Ragione sociale (persona giuridica)
- Sede legale (persona giuridica)
- P. IVA (persona giuridica)
- Codice fiscale (persona giuridica).

Attributi secondari

- Telefono mobile (persona fisica)
- Indirizzo di posta elettronica (persona fisica)
- Domicilio fisico (persona fisica)
- Data di scadenza identità
- PEC (persona giuridica).

3.4. Identificazione dell'utente



Il servizio LepidaID è disponibile per tutti i cittadini in possesso di documento di identità valido rilasciato da un'Autorità Italiana (carta d'identità, passaporto, patente di guida) oppure in possesso di carta di identità o passaporto rilasciato dalla Repubblica di San Marino.

A seguito dell'invio della richiesta di emissione di una nuova identità digitale, l'utente richiedente deve seguire un processo di identificazione che viene svolto da un operatore che svolge funzioni di Registration Authority con l'utilizzo di opportune funzionalità web a disposizione dal sistema informativo di Lepida

L'identificazione avviene secondo una delle seguenti modalità:

- Identificazione informatica tramite documenti digitali di identità di cui all'art.64 del Dlgs. n.82/2005, tra cui la tessera sanitaria-carta nazionale dei servizi (TS-CNS), CNS o carte ad essa conformi. In caso di richiesta da parte dell'utente di identificazione tramite CNS il sistema prevede apposita procedura di verifica della carta. Terminata la procedura di verifica gli estremi della sessione di log della verifica verranno salvati a sistema come dimostrazione dell'avvenuta identificazione
- Identificazione informatica tramite firma elettronica qualificata o firma digitale con l'acquisizione del modulo di richiesta di adesione in formato digitale compilato e sottoscritto con firma elettronica qualificata o con firma digitale. La verifica viene fatta automaticamente dal sistema che, dopo aver verificato la validità della firma (anche come data di scadenza) apposta sul documento provvede a confrontare il codice fiscale associato con quello dell'utente soggetto ad identificazione. Il documento firmato digitalmente viene salvato nel sistema come attestazione dell'avvenuta identificazione
- Identificazione a vista del soggetto richiedente, presso uno sportello abilitato, in occasione della quale viene effettuata una scannerizzazione fronte/retro del documento di identità e della tessera sanitaria che vengono caricati nel sistema qualora non fosse già stato fatto dall'utente durante la fase di registrazione. L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità e verifica il codice fiscale tramite la tessera sanitaria in corso di validità

- Identificazione a vista da remoto del soggetto richiedente mediante videocomunicazione web con operatore. L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità e verifica il codice fiscale tramite la tessera sanitaria in corso di validità
- Identificazione a vista da remoto tramite strumenti di registrazione audio/video nel rispetto della vigente normativa sulla protezione dei dati personali. L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile e firma autografa del richiedente stesso e verifica il codice fiscale tramite la tessera sanitaria in corso di validità. La sessione audio/video è interamente registrata e conservata per venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale con modalità crittografiche atte a garantirne l'accesso esclusivamente dietro richiesta dell'autorità giudiziaria, dell'Agenzia nel corso delle attività di vigilanza, dell'utente e dell'autorità giudiziaria in caso di disconoscimento della stessa. A dimostrazione dell'avvenuta identificazione da remoto l'operatore provvede a caricare a sistema l'intera registrazione della sessione audio/video
- Identificazione informatica tramite CIE 3.0. Il sistema prevede il collegamento al sito del Ministero dell'Interno per effettuare un'autenticazione con CIE 3.0.

Si precisa che, per gli utenti minorenni a partire dai 5 anni di età, è possibile ottenere l'identità digitale SPID LepidaID utilizzando solo l'identificazione a vista presso uno sportello abilitato e l'identificazione a vista da remoto via webcam con operatore, e che il minorenne deve essere sempre accompagnato dal genitore richiedente.

La gestione utenti, include la possibilità per gli operatori di effettuare gli interventi che si possono rendere necessari, come ad esempio il caricamento di documenti che dovessero essere stati nel frattempo ricevuti su altri canali di comunicazione, l'invio di comunicazioni secondo uno dei canali validati dall'utente (e-mail e/o SMS). Inoltre, ai soli operatori, è delegata anche la gestione delle omocodie. In tali casistiche infatti il sistema non è in grado di validare il codice fiscale immesso dall'utente sulla base delle rimanenti informazioni anagrafiche causando l'impossibilità di effettuare la registrazione. All'arrivo di segnalazioni di questa natura l'operatore dovrà accedere ad

un'area specifica dalla quale potrà identificare l'utente con il problema di omocodia e associargli il codice fiscale corretto.

3.4.1. Identificazione a mezzo webcam con operatore

Lepida mette a disposizione una modalità facoltativa di riconoscimento a mezzo webcam, e cioè l'identificazione del richiedente una identità digitale SPID LepidaID che avviene con una sessione audio/video registrata con colloquio con operatore. In ogni caso il riconoscimento non avverrà tramite strumenti automatizzati, ma sarà effettuato da un operatore attraverso l'utilizzo di strumenti informatici. Tale modalità di riconoscimento comporta, quindi, il trattamento da parte di Lepida, oltre che dei dati personali sopra indicati, anche dei dati di registrazione della voce, immagini e video dell'utente. Specificatamente le operazioni di trattamento di tali dati consistono nella registrazione del flusso audio/video relativo all'esibizione del documento di identità dell'utente e della tessera sanitaria e all'accertamento da parte dell'operatore di Lepida dell'identità del richiedente, oltre che dell'effettiva volontà dell'utente stesso di ottenere l'identità SPID fornita da Lepida.

3.4.2. Identificazione a mezzo videoregistrazione e bonifico bancario

Lepida mette a disposizione un'ulteriore modalità facoltativa di riconoscimento da remoto. L'identificazione del richiedente una identità digitale SPID può avvenire con una registrazione audio/video in cui viene dichiarata la propria identità, esibito un documento di riconoscimento e la tessera sanitaria e, infine, dichiarata l'effettiva volontà dell'utente di ottenere l'identità SPID fornita da Lepida. Tale modalità prevede anche l'esecuzione di un bonifico bancario di un importo simbolico, che può essere di importo minimo di 0,01€, da effettuarsi da un conto corrente intestato (o cointestato) al richiedente e con IBAN italiano. Il riconoscimento non avverrà tramite strumenti automatizzati, ma sarà effettuato dagli operatori di Lepida attraverso l'utilizzo di strumenti informatici. Tale modalità di riconoscimento comporta, quindi, il trattamento da parte di Lepida, oltre che dei dati personali sopra indicati, anche dei dati di registrazione della voce, della registrazione audio/video dell'utente e dei dati relativi al conto corrente intestato (o cointestato) allo stesso da cui viene effettuato il suddetto bonifico.

3.5. Amministrazione del sistema

Gli operatori di una o più sedi del gestore di identità hanno funzioni di amministrazione delle identità digitali di tutti gli utenti SPID rilasciate da Lepida, indipendentemente dalla sede da cui operano. Gli amministratori hanno funzioni di amministrazione del sistema quindi viene garantito loro l'accesso alle funzioni necessarie per la configurazione e gestione del sistema. A questi ultimi è consentito l'accesso anche all'area amministrativa suddivisa nelle seguenti sezioni: 1) Sedi: area per la configurazione delle sedi di appartenenza degli operatori. Ad ogni sede deve obbligatoriamente essere associato un ufficio; 2) Amministratori: area per l'assegnazione del ruolo di amministrazione ad utenti già registrati nel sistema; 3) Variabili: area per la configurazione delle variabili di funzionamento del sistema (ad esempio giorni validità password, etc); 4) Scheduler: componente software adibito all'esecuzione di generici task a specifiche cadenze temporali; 5) SP: area per la gestione degli SP abilitati a richiedere l'autenticazione sul sistema mediante l'IdP.

Tutti i soggetti che ricoprono le funzioni di amministratore di sistema, ai sensi e per gli effetti del Provvedimento del 27.11.2008 e ss.mm.ii. del Garante per la protezione dei dati personali, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Ciascuno di tali soggetti è nominativamente designato, con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Lepida detiene l'elenco degli amministratori designati sempre aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

3.6. Gestione dei documenti e dei log

La documentazione da conservare include le informazioni e i documenti che sono stati raccolti nel corso dell'attività di registrazione. Al fine di poter documentare la corretta esecuzione dei processi relativi all'attività di rilascio di una identità occorre conservare i riscontri relativi ai processi di identificazione e verifica. Tutta la documentazione inerente alla creazione e al rilascio di una identità digitale viene conservata ai sensi dell'articolo 7, commi 8 e 9, del DPCM 24 ottobre 2014.

Viene mantenuta traccia per ogni evento di sistema al fine di consentire una precisa

ricostruzione delle attività in caso di necessità. Verranno tracciate le seguenti tipologie di eventi:

- Autenticazioni
- Variazione dati utente
- Variazione stato
- Altri eventi.

Per tutte le tipologie di eventi verranno indicati i riferimenti temporali e, in aggiunta:

- Per gli eventi di autenticazione verranno inoltre indicati il SP e il livello SPID utilizzato;
- Per gli eventi di variazione dati verrà indicato se effettuati da operatore o dall'utente stesso. Qualora la modifica sia stata effettuata da un operatore, oltre all'identificativo dell'operatore stesso verrà inserito il link all'eventuale documentazione giustificativa dell'intervento eventualmente caricata
- Per quanto riguarda le variazioni di stato (sospensione, revoca, ecc.) verrà indicato l'eventuale operatore autore della transizione e il link all'eventuale documentazione giustificativa
- Per gli eventi di validazione verrà indicato il riferimento a tipologia e valore del contatto validato
- Per gli altri eventi generati verrà indicata la tipologia di evento verificatosi e l'eventuale azione intrapresa (es: evento di scadenza documento con azione di segnalazione all'utente tramite e-mail).

Sulla lista dei log saranno possibili filtri per tipologia evento e data nonché l'esportazione dei dati in formato CSV o PDF.

I record di log verranno salvati su database e dovranno risultare consultabili per almeno 24 mesi secondo le modalità descritte nell'art. 29 delle modalità attuative SPID. Al crescere del numero di record e al fine di salvaguardare il funzionamento del database risulta possibile prevedere procedure automatiche di svuotamento parziale della tabella di log con contestuale salvataggio su file system. Una apposita procedura dello scheduler si occuperà di eliminare selettivamente i log non più necessari basandosi su l'identificativo utente.

Considerato l'elevato numero di eventi tracciati, la gestione dello storage su database avverrà mediante sistema di code di messaggi asincrono. Sia IdP che IdM potranno aggiungere messaggi alla coda che verranno poi elaborati dal sistema in modo asincrono evitando di introdurre "colli di bottiglia" nelle procedure di runtime.

I sistemi attraverso i quali Lepida eroga il servizio IdP SPID possiedono livelli di protezione logica e fisica estremamente elevati.

I sistemi sono fisicamente allocati presso i Datacenter regionali di Lepida, a partire da quello di Ravenna, il quale è fornito di accorgimenti tecnici e procedurali che impediscono compromissioni fisiche, accessi non autorizzati e danneggiamenti dovuti ad eventi accidentali.

L'accesso ai server per qualsiasi interazione con il sistema IdP avviene mediante sistema di autenticazione e attraverso una utenza personale ed univoca esclusivamente relativa al personale incaricato.

Le tracciature previste dalla normative SPID e gli eventi registrati su ogni server che compone l'architettura del servizio IdP Lepida vengono registrati con un riferimento temporale recuperato attraverso l'abilitazione del servizio NTP (Network Time Protocol).

L'NTP rappresenta un protocollo TCP/IP che permette di sincronizzare l'ora di sistema delle macchine all'interno di una rete e, conseguentemente, di impostare il proprio orologio. Tutti gli eventi perciò vengono rilevati e memorizzati con l'orario sincronizzato e sempre corretto.

Per garantire l'integrità e la non ripudiabilità del registro delle transazioni, ad ogni tracciatura viene apposta una marca temporale da parte del servizio di gestione dei log e il registro viene inviato in conservazione sul Polo Archivistico della Regione Emilia-Romagna (ParER), soggetto accreditato presso AgID per la conservazione dei documenti informatici.

3.7. Sicurezza

Il sistema informatico è realizzato in piena compatibilità con le linee guida regionali in termini di IT governance in materia di sicurezza garantendo confidenzialità, integrità delle risorse. Vengono inoltre rispettate le linee guida di sicurezza emanate dal progetto



OWASP e riportate nell'Avviso 1 di SPID Gestione Della Sicurezza Del Canale Di Trasmissione. Il sistema garantisce la sicura identificazione dell'utente che accede alle risorse nonché la limitazione degli accessi sulla base del ruolo assegnato. Tutte le comunicazioni garantiscono un livello di sicurezza tale da non risultare alterabili da utenti esterni e al tempo stesso non permettere a terzi l'intercettazione di dati considerati sensibili. Al fine di garantire tale livello di sicurezza ad ogni canale di comunicazione verrà attribuito un grado di pericolosità. I livelli utilizzati sono: alto, medio e basso. Per ogni livello sono state definite specifiche politiche di sicurezza da implementare sul canale soggetto a tale rischio.

Le credenziali associate alle identità digitali vengono memorizzate nella banca dati del sistema con utilizzo di algoritmo di hashing robusto (SHA-256) e vengono offuscate le password nei file di configurazione delle connessioni al database.

4. Informativa agli utenti

Informativa sul trattamento dei dati personali resa ai sensi dell'art. 13 del Regolamento europeo n. 679/2016

1. Premessa

Ai sensi dell'art. 13 del Regolamento europeo n. 679/2016, sono fornite le informazioni relative ai trattamenti di dati personali effettuati da Lepida nell'ambito dell'attribuzione dell'identità digitale e di fruizione dei servizi erogati online dai "Fornitori di servizi" tramite il Sistema Pubblico per la gestione dell'Identità Digitale (SPID). Con riferimento alla conversione dell'identità pregressa del sistema di autenticazione denominato FedERa (Federazione degli Enti dell'Emilia-Romagna per l'Autenticazione) si invita a prendere visione del par. 2 del documento "LepidaID - Relazione trattamento dati personali".

2. Identità e dati di contatto del titolare del trattamento

Al fine di semplificare le modalità di inoltro e ridurre i tempi per il riscontro si invita a presentare le richieste di cui al paragrafo n. 10, a Lepida all'indirizzo dpo@lepida.it, oppure in modalità cartacea inviando la sua richiesta a Lepida in Via della Liberazione, 15, 40128 Bologna BO.

3. Il Responsabile della protezione dei dati personali

Così come previsto dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, è possibile contattare il Responsabile della protezione dei dati personali (DPO) all'indirizzo: dpo@lepida.it

4. Responsabili del trattamento

Lepida può avvalersi di soggetti terzi per l'espletamento di attività che concernono i trattamenti considerati ai fini della presente informativa. Conformemente a quanto stabilito dalla normativa, tali soggetti assicurano livelli esperienza, capacità e affidabilità



tali da garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati.

Vengono formalizzati da parte di Lepida compiti e oneri in capo a tali soggetti terzi con la designazione degli stessi a "Responsabili del trattamento".

Vengono sottoposti tali soggetti a verifiche periodiche al fine di constatare il mantenimento dei livelli di garanzia registrati in occasione dell'affidamento dell'incarico iniziale.

5. Soggetti autorizzati al trattamento

I Suoi dati personali sono trattati da personale interno previamente autorizzato e designato quale incaricato del trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta tutela dei Suoi dati personali.

6. Finalità e base giuridica del trattamento

I Suoi dati personali sono trattati per le seguenti finalità:

a) attribuzione dell'identità digitale e fruizione dei servizi erogati online dai "Fornitori di servizi" tramite il Sistema Pubblico per la gestione dell'Identità Digitale, **ivi incluse le attività di verifica sincrona della coerenza anagrafica e dell'esistenza in vita tramite i servizi di ANPR, nonché di verifica contro il furto d'identità e lo smarrimento dei documenti tramite il ws SCIPAFI;

b) gestione dell'eventuale richiesta di non attivazione dell'identità digitale. Relativamente al punto a), per l'attribuzione dell'identità digitale e fruizione dei servizi erogati online, il trattamento è necessario all'esecuzione di un contratto o all'esecuzione di misure precontrattuali (art. 6 par. 1 lett. b) del GDPR), mentre per le attività di verifica tramite i servizi indicati, il trattamento è necessario per adempiere un obbligo di legge (art. 6 par. 1 lett. c) del GDPR).

Per quanto concerne le operazioni di trattamento di cui al par. 3 la base giuridica è costituita dal consenso prestato dall'utente che richiede l'identificazione a mezzo webcam o audio/video"; in relazione all'ipotesi sub b) la base giuridica del trattamento

è costituita dal consenso dell'interessato che richiede in via preventiva la non attivazione dell'identità digitale.

7. Destinatari dei dati personali

Lepida potrà comunicare i Suoi dati personali alle seguenti categorie di soggetti:

- Dipendenti di Lepida
- Soggetti che forniscono servizi a Lepida
- Soggetti/Enti/Autorità a cui la comunicazione deve essere effettuata per adempiere a norme nazionali/europee nonché a disposizioni impartite da organi di controllo e vigilanza
- Fornitori di servizi online, al momento della richiesta di accesso ai servizi tramite la rete Internet
- Organismi di diritto pubblico / amministrazioni pubbliche quali gestori di banche dati consultate al fine di verificare la correttezza dei dati forniti dagli utenti e di prevenire i furti di identità (tra cui l'Anagrafe Nazionale della Popolazione Residente - ANPR per il tramite del sistema ERIGeN, e il Sistema Pubblico di Prevenzione delle Frodi - SCIPAFI).

8. Trasferimento dei dati personali a Paesi extra UE

I Suoi dati identificativi diretti ed eventualmente la Sua immagine non sono trasferiti al di fuori dell'Unione Europea. Per alcune operazioni di trattamento Lepida utilizza strumenti afferenti a servizi cloud qualificati dall'Agenzia per la Cybersicurezza Nazionale, in relazione ai quali alcuni dati, quelli relativi alla diagnostica e alla telemetria dei servizi, potrebbero essere trasferiti al di fuori dell'Unione Europea.

9. Periodo di conservazione

I Suoi dati personali sono trattati e conservati ai sensi dell'articolo 7, commi 8 e 9, del DPCM 24 ottobre 2014. La documentazione e i dati inerenti al processo di adesione (identificazione e verifica della identità) e i dati inerenti alla preventiva richiesta di non attivazione, sono conservati per un periodo pari a vent'anni decorrenti dalla scadenza o dalla revoca dell'identità digitale o dalla ricezione della richiesta di non attivazione dell'identità digitale o, se ricevuta in momento precedente, sino alla ricezione della

revoca del tuo consenso.

I dati relativi alle tracciatore degli accessi e delle operazioni effettuate mediante SPID (ad esempio data e ora dell'accesso, esito dell'autenticazione, indirizzo IP) sono conservati per un periodo massimo di 24 mesi dalla data della loro registrazione.

In alcuni casi, tali dati potranno essere conservati per un periodo superiore, esclusivamente quando ciò sia necessario per adempiere a obblighi di legge o per la tutela dei diritti del Titolare, anche in relazione a richieste o verifiche da parte delle Autorità competenti.

In particolare, potranno essere conservati per un periodo superiore a 24 mesi anche i dati riferibili a utenti non direttamente interessati dalle suddette attività, quando ciò si renda necessario per la corretta conservazione dei dati che, invece, costituiscono oggetto di interesse da parte della Legge, delle Autorità o la cui conservazione sia necessaria per la tutela dei diritti del Titolare del trattamento. Tale conservazione ulteriore è riferita al solo registro giornaliero delle transazioni e risulta necessaria per non compromettere l'affidabilità e il valore probatorio dei dati stessi. .

In ogni caso, tali dati sono conservati solo per le finalità sopra indicate, non sono utilizzati per ulteriori trattamenti e sono mantenuti per un periodo di tempo limitato a quanto strettamente necessario, nel rispetto dei principi di protezione dei dati personali previsti dal Regolamento (UE) 2016/679.

Si precisa che, in ogni caso, in caso di contenzioso giudiziale, i dati personali potrebbero essere conservati per tutta la durata dello stesso, fino all'esaurimento dei termini di esperibilità delle azioni di impugnazione.

Qualora non si pervenga al completamento dell'attivazione dell'identità digitale, i dati personali forniti dagli interessati nell'ambito del processo di registrazione al servizio SPID sono conservati per un periodo non superiore a 18 mesi dalla loro raccolta. Decorso tale termine, i dati personali e gli eventuali documenti acquisiti sono cancellati o anonimizzati, nel rispetto del principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e) del Regolamento (UE) 2016/679.

10. I suoi diritti



Nella sua qualità di interessato, Le sono riconosciuti i diritti esplicitati ai sensi degli artt. 15 e ss. del Regolamento UE n. 679/2016, in particolare :

- Di accesso ai dati personali
- Di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che la riguardano
- Di opporsi al trattamento
- Di proporre reclamo al Garante per la protezione dei dati personali.

11. Conferimento dei dati

Il conferimento dei Suoi dati è facoltativo, ma necessario per le finalità sopra indicate. Il mancato conferimento comporterà l'impossibilità di dare seguito alla sua richiesta di Identità Digitale SPID LepidaID e di fruizione dei servizi erogati online dai "Fornitori di servizi" tramite il Sistema Pubblico per la gestione dell'Identità Digitale.