IdP Lepida SpA - Informativa inerente i rischi derivanti dal possesso dell'identità digitale SPID

Sommario

1. Introduzione

1.1 Storia del documento

Versione	Data	Cambiamenti apportati
1.0	21/12/2017	Prima stesura
1.1	30/03/2018	Aggiornamento
1.2	11/07/2018	Aggiornamento Informativa e aggiunto paragrafo "Cautele e contromisure"

1.2 Scopo del documento

Il presente documento elenca le informazioni fornite ai titolari dell' identità digitale SPID inerenti i rischi derivanti dal possesso della stessa, le cautele e le contromisure adottabili degli stessi.

2. Informativa

Di seguito l'elenco degli obblighi e delle responsabilità che vengono inseriti nel modulo di adesione a SPID che il titolare dell'identità deve sottoscrivere all'atto della richiesta delle identità digitale:

- Il Titolare dichiara di assumersi la responsabilità, ai sensi dell'articolo 76 del decreto del Presidente della Repubblica 28 dicembre 2000, n.445, della veridicità delle informazioni fornite.
- Il Titolare dichiara di aver preso visione dell'Informativa ai sensi dell'art. 13 del D.Lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali" disponibile all'indirizzo: https://id.lepida.it .
- Il Titolare dichiara di aver preso visione del Manuale Operativo e della Guida Utente disponibili all'indirizzo all'indirizzo https://id.lepida.it .
- Il Titolare dichiara di accettare, in qualità di Titolare di identità digitale SPID, tutte le clausole e le condizioni riportate nel documento Modulo Adesione a SPID che costituisce a tutti gli effetti un Contratto.
- Il Titolare di Identità si impegna a fornire a LepidaSpA tutte le informazioni richieste ai fini dell'esecuzione del Servizio LepidaID e dei necessari controlli nonché a notificare, con le modalità indicate nel Manuale Operativo, ogni variazione dei dati comunicati.
- Nei limiti massimi consentiti dalla legge, il Titolare dell'Identità Digitale si assume, inoltre, qualsivoglia responsabilità, in ordine all'utilizzo improprio delle Credenziali o all'utilizzo delle stesse con forme e modalità difformi dalla normativa vigente e dal Manuale Operativo, impegnandosi ad esonerare LepidaSpA da qualsiasi pretesa o azione da parte di terzi.
- Il Titolare dell'Identità Digitale si obbliga a non utilizzare le Credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi o regolamenti. A tal proposito, si precisa che il Titolare dell' Identità Digitale è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.
- Il Titolare, garantisce la veridicità di tutti i dati personali comunicati in occasione dell'identificazione e validazione del numero di telefono cellulare, in quanto consapevole che chiunque renda dichiarazioni mendaci è punibile ai sensi del codice penale e delle leggi speciali in materia (DPR 445/2000).
- Il Titolare all'atto della richiesta del servizio, dichiara di aver preso attenta visione delle presenti Condizioni e dei documenti ivi richiamati, di averne compreso a pieno il contenuto e di essere edotto;
- Il Titolare ha l'obbligo dell'utilizzo esclusivamente personale delle credenziali connesse all'Identità Digitale oltre che l'onere a suo carico di provare che le medesime sono state abusivamente utilizzate da terzi;
- Nei limiti massimi consentiti dalla legge, il Titolare si assume, inoltre, qualsivoglia responsabilità, in ordine all'utilizzo improprio delle Credenziali o all'utilizzo delle stesse con forme e modalità difformi dalla normativa vigente e dal Manuale

Operativo, impegnandosi ad esonerare LepidaSpA da qualsiasi pretesa o azione da parte di terzi.

- Il Titolare si obbliga a non utilizzare le Credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi o regolamenti; si precisa quindi che il Titolare è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.
- Il Titolare, in particolare, è obbligato:
    - all'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private;
    - a sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle Credenziali e fornire tempestivamente a LepidaSpA, comunque entro 30 giorni, copia di detta denuncia;
    - a mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti Attributi relativi alla propria persona fisica: estremi del documento di riconoscimento e relativa scadenza, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale;
    - a conservare le Credenziali e le informazioni per l'utilizzo dell'Identità digitale in modo da minimizzare i rischi di divulgazione, rivelazione, manomissione, furto, duplicazione, intercettazione, cracking dell'eventuale token associato all'utilizzo dell'identità digitale;
    - ad accertarsi dell'autenticità del Fornitore di servizi o del Gestore dell'Identità digitale quando viene richiesto di utilizzare l'Identità digitale;
    - a conservare con la massima diligenza le Credenziali che gli sono state attribuite, impegnandosi altresì a non consentire l'utilizzo del Servizio a terzi;
    - a richiedere, secondo le modalità previste nel Manuale Operativo, l'immediata sospensione e la successiva revoca delle Credenziali nei casi previsti.
- Il Titolare si obbliga, altresì, a non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge o dalla consuetudine. In caso di violazione di una delle presenti disposizioni, LepidaSpA potrà risolvere il presente contratto senza necessità di dare preavviso, né tanto meno, sarà tenuta a risarcire alcun danno, fatta salva ogni eventuale azione di rivalsa nei riguardi dei responsabili delle violazioni.
- Laddove la verifica dell'identità del Richiedente avvenga nei modi previsti dall'art. 7, comma 2, lett. b), d), ed e) del citato DPCM 24 ottobre 2014, i dati personali che saranno inseriti nel modulo di richiesta di adesione al Servizio LepidaID saranno quelli contenuti nella banca dati corrispondente a ciascuno strumento utilizzato. Pertanto il sottoscritto, con la richiesta del Servizio LepidaID e l'accettazione del Contratto autorizza espressamente detto trattamento dei propri dati personali affinché siano utilizzati quali Attributi Identificativi ed eventualmente quali Attributi secondari, confermandone la validità e correttezza.
- Il Titolare, fino all'effettiva eventuale sospensione o revoca o recesso del/dal Servizio, è direttamente e esclusivamente responsabile di tutti gli atti posti in essere utilizzando le Credenziali.

3. Cautele e contromisure

In questo paragrafo vengono riportati consigli e buone pratiche da adottare da parte del Titolare per ridurre i rischi di violazione ed abusi relativamente all'Identità Digitale dello stesso.

Dati e password

- **Memorizzazione dati di contatto personali**
  - Il Titolare deve memorizzare indirizzo email e telefono cellulare, dati associati all'identità digitale, in quanto in caso di smarrimento l'identità digitale risulterebbe inutilizzabile.
- **Non ri-utilizzo della password**
  - Non riutilizzare la stessa password per account differenti in quanto scoperta la password sarebbero violati tutti gli account compreso quello relativo all'identità digitale.
- **Cambio password**
  - Cambiare regolarmente la password per rendere sicuro l'accesso. Il software obbliga il cambio password ogni 6 mesi.
- **Conservazione password**
  - Conservare la password in luogo sicuro in modo che l'informazione non possa essere sottratta da altri.
- **Verifica dell'utilizzo della mail**
  - Il Titolare ogni volta che utilizza la propria identità digitale potrà ricevere nel caso il attivi il controllo una mail di notifica, in modo che si possa così accorgere di eventuali usi impropri.

Dispositivo cellulare / smartphone

- **Blocco schermo cellulare**
  - E' consigliabile che il Titolare imposti il blocco schermo sul cellulare (blocco tramite pwd, pin numerico ecc..), in modo che in caso di furto/smarrimento un ipotetico malintenzionato non possa accedere.
- **Disattivazione anteprima SMS**
  - E' opportuno che il Titolare configuri l'inibizione dell'anteprima dei messaggi in modo che nessuno possa leggere il codice di accesso allo SPID.
- **Aggiornamento dispositivo**
  - Il dispositivo cellulare dovrà essere mantenuto aggiornato sia lato sistema operativo che relativamente agli aggiornamenti delle applicazioni installate, per evitare l'accesso di malintenzionati al dispositivo.
- **Applicazioni provenienti solo dai market ufficiali**
  - E' consigliato installare solamente applicazioni provenienti dai market ufficiali.
- **Resettare smart phone quando non è più utilizzato**
  - E' consigliabile che il Titolare effettui il ripristino dei dati di fabbrica del dispositivo in caso di dismissione.

Smart card

- **Smart Card (CE o CNS)**
  - Evitare di conservare la smart card nello stesso luogo dove si conserva il relativo PIN.
  - Evitare di reimpostare il PIN della smart card ad un nuovo valore basato su schemi prevedibili.

Computer (PC)

- **Antivirus e Firewall**
  - Attivare la protezione della postazione PC attraverso software antivirus e personal firewall.
  - Impostare il PC in modo che l'antivirus e firewall siano sempre attivi all'avvio.
- **Aggiornamento software**
  - Attivare l'aggiornamento automatico del sistema operativo della postazione.
- **Logout identità digitale ed eliminazione tracce**
  - Nel caso si utilizzi l'identità digitale utilizzando computer pubblici ricordarsi di effettuare il Logout dell'identità digitale oltre che cancellare utilizzando le funzionalità lato browser per cancellare i dati relativi ai moduli, password, cache e cookie.

Violazione accesso o uso improprio della credenziali

Nel caso di violazione si possono verificare, a titolo indicativo e non esaustivo, le seguenti conseguenze :

1. impossibilità di accesso;
2. ricezione di notifiche (se attivato il controllo da parte dell'utente) di utilizzo senza che ci sia stato utilizzo;
3. ricezione notifica di variazione numero telefono o mail, che l'utente in realtà non ha variato.

In caso di violazione dell'accesso, il Titolare deve richiedere a Lepida la revoca o la sospensione della proprio identità digitale secondo le modalità descritte nel Manuale Operativo.
Si sottolinea che la tempestiva comunicazione e sospensione della violazione dell'accesso permettono di evitare o ridurre i rischi per il Titolare derivanti da un utilizzo improprio dell'identità in termini di accesso illegittimo a servizi e di possibili danni, truffe o frodi.