economiesuisse

Protezione dei dati: una panoramica della nuova legge

Nell'autunno 2020 il Parlamento ha adottato la nuova legge sulla protezione dei dati. Il termine per un referendum è scaduto nel gennaio 2021 e non è stato lanciato alcun referendum. Dal momento che i lavori relativi all'ordinanza d'esecuzione (OLPD) sono ancora in corso, la nuova legge potrebbe entrare in vigore nel secondo semestre 2022.

Per le imprese svizzere è consigliabile familiarizzare da subito con la nuova legge e le sue esigenze e di adeguare il proprio dispositivo di protezione dei dati, in particolare per quanto concerne le disposizioni relative alla protezione dei dati e contratti. economiesuisse risponde alle questioni più urgenti in collaborazione con due avvocati, Cornelia Stengel e Luca Stäuble allo scopo di segnalare alle imprese svizzere le misure da adottare in relazione all'entrata in vigore della nuova legge sulla protezione dei dati (LPD).

Il presente giro d'orizzonte ha l'unico scopo di informare e sensibilizzare le persone interessate. Esso non sostituisce una consulenza giuridica. economiesuisse non potrà essere ritenuta responsabile per le azioni od omissioni conseguenti alla lettura di questo testo.

FAQ

1) Quali sono lo scopo e il campo d'applicazione della nuova legge sulla protezione dei dati?

La nuova legge sulla protezione dei dati mira a proteggere la personalità e i diritti fondamentali delle persone fisiche residenti in Svizzera e i cui dati sono oggetto di un trattamento da parte di privati (società private) o dallo Stato. I dati delle persone giuridiche non saranno protetti maggiormente. L'idea è quella di offrire alle persone interessate una maggiore trasparenza e di rafforzare i loro diritti sui loro dati personali («autodeterminazione informativa»). La nuova legge mira anche a promuovere le misure di prevenzione e la responsabilità individuale dei responsabili del trattamento dei dati. Per poterlo fare, la legge rafforza la sorveglianza della protezione dei dati e sviluppa le disposizioni penali. Essa introduce anche nuovi obblighi per le imprese, in particolare in caso di rilevamento, perdita o utilizzo abusivo di dati personali.

2) Dove si applica la nuova legge?

Benché la nuova LPD sia prevista per il territorio svizzero, essa ha anche una portata extraterritoriale. In particolare, può estendersi a circostanze che si verificano all'estero ma che hanno ripercussioni in Svizzera (art. 3). In altre parole, se il processo di trattamento di dati personali ha luogo al di fuori della Svizzera, ma concerne persone fisiche residenti in Svizzera e produce degli effetti in Svizzera (questo criterio dovrebbe essere precisato nell'ordinanza), il responsabile del trattamento dei dati in questione è tenuto a rispettare la nuova legislazione svizzera. Esso deve inoltre nominare, a determinate condizioni, un rappresentante legale in Svizzera (art. 14 e 15 nuova LPD).

Esempio: un'impresa con sede all'estero e che tratta i dati delle persone fisiche residenti in Svizzera dall'estero. In questo caso, occorre valutare singolarmente ogni situazione. La nuova LPD si applica se il trattamento di dati in Svizzera è «sensibile». Ad esempio, il RGPD esamina se dei dati sono trattati allo scopo di concepire un'offerta di beni o di servizi destinati a persone in seno all'UE.

3) Per quale motivo si rende necessaria una revisione della legge attuale?

L'attuale legge svizzera sulla protezione dei dati risale al 1992. In seguito, il trattamento e l'utilizzo di dati personali sono cresciuti man mano che l'economia e la società si sono digitalizzati. A livello mondiale e in particolare in seno all'UE, la protezione dei dati è stata considerevolmente rafforzata e le organizzazioni internazionali hanno inasprito le loro norme minime in materia. Per la Svizzera, si è dunque reso necessario adattare la sua legge del 1992 alle nuove abitudini di consumo (acquisti online, reti sociali, ecc.), agli sviluppi tecnologici (digitalizzazione, intelligenza artificiale, ecc.) e alle norme internazionali.

Adottando il suo regolamento generale sulla protezione dei dati (RGPD), l'Unione europea ha creato un nuovo standard a livello internazionale. Entrato in vigore il 25 maggio 2018, questo regolamento fa parlare di sé in tutto il mondo a causa della sua portata extraterritoriale. Numerose imprese svizzere rientrano nel campo d'applicazione del RGPD, a seguito del loro orientamento sui mercati dell'UE o dello SEE. A ciò va aggiunto che il RGPD prevede che si possano trasferire dati verso un altro Stato unicamente se quest'ultimo presenta un livello di protezione dei dati «adeguato» dal punto di vista dell'UE. Una circolazione dei dati fluida proveniente dall'UE è particolarmente importante per paesi come la

Svizzera, che intrattengono relazioni economiche molto strette con l'UE stessa.

Un obiettivo importante della revisione della LPD è dunque quello di elaborare una soluzione coordinata a livello internazionale – «equivalente» dal punto di vista dell'UE – che promuova gli sviluppi tecnologici in relazione all'economia dei dati e che, nel contempo, non abbandoni i punti di forza della legislazione precedente.

La nuova legge sviluppa in particolare gli obblighi in materia d'informazione e i diritti delle persone interessate. Essa regola anche ciò che viene definito «profilazione». Quest'ultima copre ogni genere di trattamento automatizzato dei dati personali allo scopo di valutare, analizzare o prevedere il comportamento di una persona fisica (in particolare il rendimento al lavoro, la situazione economica, la salute, gli interessi, la localizzazione). Conseguenze giuridiche più rigide si applicano unicamente in caso di profilazione che presenta un rischio elevato per la personalità dell'interessato.

Dal punto di vista dell'UE la Svizzera dispone di un livello di protezione dei dati «adeguato»?

Dal punto di vista dell'UE la Svizzera è un «paese terzo». Affinché il trasferimento di dati verso un paese terzo sia possibile, è necessaria una decisione della Commissione europea relativa all'adeguatezza del dispositivo svizzero. La Svizzera dispone di una simile decisione, ma quest'ultima si basa sulla vecchia legislazione europea. L'UE sta attualmente esaminando se la nuova LPD sia adeguata rispetto al RGPD. Con la revisione, la Svizzera avrebbe dovuto creare le condizioni perché l'UE confermasse l'adeguatezza. A causa dell'ultima giurisprudenza dell'UE sui flussi di dati verso paesi terzi, ma probabilmente anche per ragioni politiche, l'adozione della risoluzione annunciata per l'anno scorso è stata rinviata.

Infine, non bisogna dimenticare che la modernizzazione del diritto svizzero si iscrive in un contesto internazionale dove i cittadini e i consumatori di tutto il mondo chiedono una migliore protezione dei loro dati personali e un maggiore controllo di questi ultimi. Questa tendenza non si osserva unicamente nell'UE, ma in numerosi paesi, tra cui il Giappone. La California ha inasprito la propria legislazione in materia di protezione dei dati, basandosi parzialmente sulla norma europea.

4) Quando entrerà in vigore la nuova LPD?

Molto probabilmente, la nuova LPD entrerà in vigore nel secondo semestre 2022. Tuttavia, poiché i lavori sulle ordinanze non sono ancora terminati (consultazione prevista per giugno 2021), questa data non è ancora stata confermata e alcune fonti partono dal presupposto di un'entrata in vigore più tardiva. Tuttavia, la legge non prevede periodi di transizione rilevanti, motivo per cui le imprese devono attuare gli adeguamenti necessari in tempo utile.

5) In quali ambiti la nuova legge svizzera va più lontano del RGPD europeo?

La nuova LPD si ispira al RGPD, ma presenta alcune caratteristiche particolari. Nella maggior parte dei casi, la legge svizzera è meno formalista e ha esigenze minori rispetto al RGPD. Vi sono però alcuni punti dove la nuova legge svizzera sarà più severa del RGPD. Si tratta in particolare del campo d'applicazione

materiale (art. 2 nuova LPD), del dovere d'informazione in occasione del trattamento di dati personali (art. 19 nuova LPD), delle multe per le persone fisiche (art. 60 ss. nuova LPD) e della definizione dei dati personali particolarmente sensibili.

6) La nuova legge esclude le PMI? Saranno interessate solo le grandi imprese?

No. Tutte le imprese, senza eccezioni, sono interessate dalla nuova LPD. Indipendentemente dalla sua dimensione, un'impresa possiede numerosi dati sui suoi clienti, partner, fornitori e collaboratori. Con la digitalizzazione dell'economia, la quantità di dati da elaborare nelle aziende, comprese le PMI, continuerà ad aumentare. Di conseguenza, tutte le imprese dovrebbero prepararsi all'entrata in vigore della nuova legge. Poiché la legge si basa sulle norme dell'UE, questo vale a maggior ragione per le aziende che non hanno ancora adattato il loro concetto di protezione dei dati al RGPD.

Inoltre, occorre considerare il fatto che la criminalità nello spazio digitale è in costante aumento. Il numero di cyberattacchi aumenta e nessuna impresa è al riparo. La nuova legge sulla protezione dei dati impone alle imprese di adottare le necessarie misure organizzative e tecniche per garantire la sicurezza dei dati ed evitare per quanto possibile il loro utilizzo abusivo.

7) Cosa dovranno fare le imprese per essere conformi?

Ogni impresa deve prepararsi all'entrata in vigore della nuova legge. Per determinare i requisiti di conformità sono necessari un censimento dei dati personali trattati in seno all'impresa e una valutazione dei rischi. Inoltre, il lavoro di implementazione necessario può essere identificato mediante un'analisi delle lacune (confronto dello stato attuale e dell'obiettivo). Esistono requisiti di conformità più elevati ad esempio quando:

- Le imprese trattano un gran volume di dati personali. Esempio: delle società specializzate nella vendita online o nell'import/export hanno un notevole potenziale di clienti che generano un conseguente volume di dati personali.
- Le imprese trattano dati personali particolarmente sensibili (ai sensi dell'art. 5 nuova LPD). Esempio: sono interessate le imprese che trattano dati personali relativi alle opinioni politiche, religiose, alla salute, ai dati genetici, razziali, all'aiuto sociale, ai perseguimenti penali, alla profilazione, ecc.

In questi casi le esigenze relative al trattamento lecito dei dati personali o il rischio di violazione dei diritti della personalità sono più elevati che non nel caso di imprese che trattano i dati di un numero limitato di collaboratori, di fornitori, di clienti, ecc.

A seconda del tipo e del volume dei dati personali trattati, il lavoro di conformità alla protezione dei dati richiede lo sviluppo o la consultazione di competenze in materia di protezione dei dati, nonché l'istituzione di processi interni al fine di soddisfare i requisiti della nuova legge. Da non sottovalutare sono le risorse materiali (software di gestione dei dati, ecc.), le risorse umane (responsabile della

protezione dei dati o impiegati responsabili della protezione dei dati, ecc.).

A seconda dell'ampiezza dei requisiti di conformità, le imprese sono vivamente invitate a ricorrere ai servizi di esperti in informatica e di avvocati nonché alle formazioni proposte dalle Camere di commercio.

8) Perché è importante prepararsi al più presto?

Ad eccezione di alcuni obblighi, la nuova legge non prevede un termine di transizione per conformarsi. Così, una gran parte dei doveri delle imprese iscritti nella legge si applicheranno dall'entrata in vigore della nuova LPD. È importante e raccomandato prepararsi con largo anticipo e identificare da subito le eventuali misure da adottare. Per essere sicuri che quando entrerà in vigore la nuova LPD sia garantita un'efficace protezione dei dati, si possono già da subito intraprendere alcune azioni (sviluppo tempestivo di competenze interne, creazione di linee guida interne e adattamento di documenti come le dichiarazioni in materia di protezione dei dati e i contratti con partner e responsabili del trattamento dei dati).

9) Quali sono i principali cambiamenti rispetto alla legge attuale?

La nuova legge introduce nuovi obblighi per le imprese. I principali sono:

- garantire la protezione dei dati attraverso la tecnologia e le impostazioni predefinite favorevoli alla protezione dei dati, in particolare in modo che i principi di trattamento siano rispettati e il trattamento dei dati sia limitato al minimo necessario per lo scopo di utilizzo (art. 7 nuova LPD);
- creare e mantenere un registro delle attività di trattamento dei dati. Le imprese che contano meno di 250 collaboratori beneficiano di un'eccezione, ma soltanto se il loro trattamento dei dati comporta un rischio basso di attacco alla personalità delle persone interessate (questo sarà precisato nell'ordinanza, art. 12 nuova LPD);
- obbligo di informare l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) e la persona interessata in caso di violazione della sicurezza dei dati (art. 24 nuova LPD);
- effettuare un'analisi d'impatto relativa alla protezione dei dati personali quando il trattamento dei dati presenta un rischio elevato (art. 22 nuova LPD);
- informare in caso di trattamento dei dati e indicare il nome del o degli Stati in caso di comunicazione all'estero (art. 19 nuova LPD). Su questo punto, la nuova LPD è più severa del RGPD;
- informare in caso di decisione individuale automatizzata – vale a dire una decisione presa nei confronti di una persona, mediante algoritmi applicati ai suoi dati personali senza che nessun essere umano intervenga nel processo (art. 21 nuova LPD).

10) Quali sono i nuovi diritti delle persone private?

L'obiettivo principale di questa legge è quello di rafforzare la trasparenza e la protezione dei dati personali delle persone interessate. In tale ottica, le persone private beneficeranno dei nuovi seguenti diritti:

- il diritto di essere informati del trattamento dei propri dati personali (art. 25-27 nuova LPD);
- il diritto alla trasmissione dei dati personali (portabilità dei dati) (art. 28 e 29 nuova LPD);
- il diritto di non essere oggetto di una decisione individuale automatizzata – vale a dire una decisione presa nei confronti di una persona, mediante algoritmi applicati ai suoi dati personali senza che nessun essere umano intervenga nel processo (art. 21 nuova LPD).

11) Quali sono gli altri cambiamenti rispetto alla legge attuale?

Gli altri cambiamenti rispetto alla legge attuale sono i seguenti:

- Dati personali: questa nozione è ormai ridotta poiché non comprende più i dati delle persone giuridiche escludendo queste ultime dal campo di protezione della LPD (art. 1 e art. 5, lett. a nuova LPD).
- Dati personali sensibili: essi includono ora i dati genetici e biometrici (che permettono un'identificazione unica) (art. 5, lett. c nuova LPD).
- Responsabile del trattamento: esso corrisponde all'attuale «detentore di una collezione di dati» e al «responsabile del trattamento» secondo il RGPD. Si tratta di una persona privata (spesso un'impresa) o di un organo federale che, solo o congiuntamente con altri, determina le finalità e i mezzi di trattamento dei dati personali (art. 5, lett. j nuova LPD).
- Extraterritorialità: estensione del campo d'applicazione della nuova LPD a circostanze che si verificano all'estero e che hanno ripercussioni in Svizzera (art. 3, cpv. 1 nuova LPD).
- Nomina di un rappresentante in Svizzera per imprese estere: questo obbligo si applica se un responsabile del trattamento privato ha la sua sede o il suo domicilio all'estero, tratta dati personali di persone in Svizzera e sono soddisfatte ulteriori condizioni (art. 14 f. nuova LPD).

12) Quali sono i rischi incombenti in caso di mancato rispetto della legge?

In caso di violazione della nuova legge, si rischiano multe fino a 250'000 franchi. Contrariamente al RGPD, le sanzioni previste dalla nuova LPD non sono rivolte all'impresa colpevole, bensì alla persona fisica incaricata della protezione dei dati (ad esempio direttore o membro del consiglio d'amministrazione). Viene punito soltanto un comportamento che potrebbe essere ritenuto intenzionale (art. 60 ss. nuova LPD).

13) Qual è la posta in gioco per le imprese?

Ignorare la (nuova) legge sulla protezione dei dati può avere conseguenze non solo per il responsabile in seno ad un'impresa, ma anche per l'impresa stessa, in particolare la sua reputazione. L'incaricato federale della protezione dei dati (IFPDT) può intervenire e prendere delle misure amministrative (ad esempio ordinare la modifica, la sospensione o la cessazione di un trattamento o la cancellazione di dati personali).

14) Come prepararsi ai cambiamenti?

Innanzitutto, è necessario prepararsi il prima possibile, e questo attraverso un'analisi delle lacune allo scopo di adattarsi passo dopo passo a questo nuovo regime regolamentare. Secondo la dimensione dell'impresa, ciò può richiedere diversi mesi. Sono però necessarie soluzioni pragmatiche, vale a dire che bisogna iniziare con l'attuare i requisiti minimi obbligatori per legge (un registro, l'obbligo di informare, ecc.).

15) Come definire un piano d'azione?

Un piano d'azione dovrebbe basarsi sui seguenti tre pilastri: sicurezza informatica, aspetti giuridici e gestione dei dati. A proposito dell'ultimo punto, economiesuisse ha messo a disposizione una carta dell'economia svizzera per una gestione responsabile dei dati. Se necessario, le aziende dovrebbero consultare esperti di sicurezza informatica e protezione dei dati per sviluppare programmi di compliance dettagliati che soddisfino i nuovi requisiti.

16) Di quali principi bisogna tener conto? E quali azioni sono richieste?

Senza entrare nelle considerazioni tecniche, giuridiche e informatiche di una conformità con la nuova LPD, un piano d'azione pragmatico dovrebbe considerare i seguenti aspetti:

1. **È necessario un punto della situazione globale**
   Secondo la nuova LPD, le imprese devono rispettare alcuni obblighi di informazione, cioè devono fornire informazioni sull'identità del controllore, lo scopo del trattamento, gli eventuali destinatari dei dati, ecc. quando ottengono dati personali. Inoltre, devono essere in grado di soddisfare i diritti degli interessati, come ad esempio fornire a un interessato informazioni sul trattamento dei suoi dati personali. Tutto questo presuppone che le aziende sappiano quali dati personali sono trattati per quali scopi, se i dati sono trasferiti ad altri paesi e ad altre persone, ecc. Di conseguenza, le imprese dovrebbero prima fare un inventario di tutto il trattamento dei dati. Il nuovo elenco richiesto dalla legge può servire come modello per questo. Tale inventario è uno sforzo collettivo che deve coinvolgere tutti i dipendenti coinvolti nel trattamento dei dati personali.
2. **Valutare i rischi**
   Più il volume di dati personali trattati da un'impresa è importante e più i dati personali sono sensibili, più le esigenze di conformità in materia di protezione dei dati sono elevate e più le potenziali sanzioni e gli attacchi alla reputazione in caso di mancato rispetto sono elevati (cf. questione 6).
3. **Sensibilizzare**
   Indipendentemente dalla dimensione dell'impresa, tutti i collaboratori, dagli apprendisti agli amministratori, devono essere sensibilizzati sulla posta in gioco in materia di protezione dei dati. I ricezionisti, i responsabili di progetti, i responsabili delle risorse umane, i consulenti, gli indipendenti, il capo impresa – collaboratori a tutti i livelli di un'impresa trattano regolarmente dati personali assumendone la responsabilità sul piano penale. Esempio: un ricezionista tiene un registro dei visitatori di

un'impresa. Trattando e archiviando i nomi delle persone che giungono nell'impresa, quest'ultimo tratta già dei dati personali.

4. **Trasparenza e informazione**
   Con la nuova LPD la trasparenza in materia di trattamento dei dati resta un principio importante. Esiste pure l'obbligo di informazione in caso di trattamento dei dati. Il responsabile del trattamento è tenuto ad informare le persone interessate dei vari aspetti del trattamento di dati. L'allestimento e l'aggiornamento della dichiarazione in materia di protezione dei dati sono essenziali in vista dell'entrata in vigore della nuova LPD (sul sito web dell'impresa, ma anche nella corrispondenza).
5. **Sicurezza informatica**
   Le imprese devono accertarsi che la sicurezza dei sistemi informatici dell'impresa e delle applicazioni di software rispondano alle esigenze della nuova legge. Ciò comprende misure tecniche ed organizzative per prevenire i cyberattacchi, il furto di dati e altre perdite di dati.
6. **Organizzazione e procedure interne**
   Allo scopo di rispondere conformemente alle esigenze della nuova legge, agli eventuali solleciti esterni (domande d'informazione o di cancellazione dei dati personali di un cliente) o agli incidenti che comportano la fuga, la perdita o l'utilizzo abusivo di dati personali, occorre stabilire procedure interne adattate alla struttura di ogni impresa. Secondo l'incidente, queste procedure devono definire quale collaboratore (supplenti inclusi) deve adottare quale misura entro quale termine. Esempio: nel caso di una violazione della sicurezza dei dati, le procedure devono stabilire le situazioni e i criteri che permettono di valutare se un incidente debba essere segnalato alle autorità. Queste procedure devono inoltre comportare spiegazioni chiare che indichino quale collaboratore deve segnalare l'incidente, entro quale termine, sotto quale forma e a quale autorità. Questo genere di procedure può assumere la forma di liste di controllo (check-list).
7. **Stabilire un registro delle attività**
   La nuova LPD prevede che sia il responsabile del trattamento che l'incaricato debbano tenere un registro delle loro attività. Questo obbligo concerne tutte le imprese. Il Consiglio federale può però prevedere delle eccezioni per le imprese con meno di 250 collaboratori (art. 12, cpv. 2 nuova LPD). Queste eccezioni saranno precisate nell'ordinanza, il cui progetto è ancora in fase di elaborazione. L'allestimento di tali registri presuppone che tutti i trattamenti di dati personali in seno ad un'impresa siano identificati e compilati sistematicamente. Soprattutto nei casi in cui non si tengono ancora elenchi corrispondenti e si effettuano molte elaborazioni diverse, questo processo comporta uno sforzo considerevole e dovrebbe quindi essere affrontato in una fase iniziale.
8. **Revisione dei contratti**
   Considerati i cambiamenti che si opereranno con la nuova legge ed entro la sua entrata in vigore, le imprese dovrebbero esaminare – e se necessario, adattare – i contratti stipulati con i loro clienti, fornitori, operatori di servizi ma anche con i loro collaboratori. Ciò richiede del tempo. È opportuna anche una attuazione rapida, poiché bisogna attendersi che numerosi partner contrattuali esigano nei mesi futuri dei contratti – o adattamenti ai contratti già esistenti – che includano clausole conformi alla nuova legge sulla protezione dei dati.

9. **Restare informati**
   Per comprendere il tema della conformità alla protezione dei dati, secondo la nuova LPD, è necessario essere in grado di capire l'impatto specifico della nuova legge sulle proprie operazioni di trattamento dei dati. Informatevi consultando i siti delle autorità di protezione dei dati (IFPDT), i blog e le riviste specializzate e partecipate alle diverse formazioni (proposte, ad esempio, dalle Camere di commercio).