BOSS conoscenza applicata
NEWSLETTER LAVORO
Aprile 2023

Come prepararsi all'entrata in vigore della nuova Legge

La nuova Legge sulla Protezione dei Dati (nLPD)

Roberta De Giusti (Country Manager di Privacy Desk Suisse SA)

Quali sono le basi che hanno ispirato la revisione della LPD?
La revisione della LPD nasce dall'esigenza di modernizzare la Legge del 1992 affinché sia al passo con l'evoluzione tecnologica, che propone grandi sfide per la protezione dei dati, e di continuare a garantire la compatibilità con il diritto vigente fuori dal territorio della Confederazione Elvetica. In particolare, con il Reg. UE 2016/679 (GDPR) che prevede che si possa procedere con un trattamento transfrontaliero verso Stati terzi a condizione che questi presentino un livello di protezione adeguato. In tal modo è garantita la libera circolazione dei dati. La Svizzera ha beneficiato fino ad oggi di un riconoscimento di adeguatezza (in corso di revisione) rientrando tra questi Paesi.

Quali i principi generali della versione finale che sta per entrare in vigore?
I principi generali previsti dalla nLPD sono vicini ai principali istituti del GDPR e differiscono per tipicità svizzera solo per alcuni aspetti. Facendo una sintesi degli istituti innovativi della nLPD possiamo indicare: l'estensione dell'obbligo di informazione, informativa privacy agli interessati, prima previsto per specifici trattamenti (per i privati); la previsione di un consenso espresso in caso di trattamento di dati degni di particolare protezione e profilazione ad alto rischio; la previsione della notifica di data breach all'Incaricato Federale per la protezione dei dati (IFPDT) e la comunicazione agli interessati; l'obbligo del registro delle attività di trattamento dei dati (tranne per le aziende con meno di 250 dipendenti); l'obbligo di effettuare una valutazione d'impatto quando il trattamento previsto presenta un rischio elevato per la personalità e i diritti fondamentali della persona interessata; la necessità di determinare una tempistica di conservazione dei dati e/o definire un criterio per la conservazione dei dati stessi.

Quale rapporto esiste fra nuova LPD e GDPR europea?
Il GDPR e la nLPD sono strettamente connessi l'uno all'altra proprio perché la nLPD trae profonda ispirazione dal GDPR. In termini operativi le aziende che trattano dati in Svizzera ma che, nell'ambito delle attività d'impresa "sconfinano", offrendo servizi e/o prodotti ad interessati nell'UE devono ragionare e valutare l'attrattività della normativa UE. In sostanza deve essere valutata attentamente l'applicabilità delle previsioni dell'art. 3 par. 2 del GDPR relative all'ambito di applicazione territoriale. Il GDPR si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, anche se è effettuato da un Titolare o da un Responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento, effettuate dalla società che opera in Svizzera, riguardano l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'UE. L'attrattività è valutata mediante una serie di parametri meglio descritti nel consideranda 23 del GDPR. È importante ricordare che anche la nLPD è attrattiva poiché prevede all'art. 3 par. 1 che la legge si applichi alle fattispecie che generano effetti in Svizzera, anche se si verificano all'estero.

Come si configurano le responsabilità per i diversi organi (addetti, manager, membri CdA)?
La nLPD si basa principalmente su un regime sanzionatorio di tipo penale. Possiamo dire, in linea generale, che rispondono dei reati commessi solo le persone fisiche. Tuttavia, in via d'eccezione, la nLPD individua dei casi in cui può rispondere l'azienda. Tale scenario presuppone l'individuazione delle persone che sono considerate responsabili penalmente, ossia il padrone d'azienda, il datore di lavoro, il mandante o la persona rappresentata o gli organi, i membri degli organi, i soci preposti alla gestione, le persone effettivamente dirigenti o i liquidatori colpevoli. Per meglio contestualizzare quanto sopra detto è importante richiamare l'art. 64 della nLPD che dispone che alle infrazioni commesse nell'azienda sono applicabili gli artt. 6 e 7 della legge federale sul diritto penale amministrativo (DPA). Capiamo ora cosa dicono gli artt. 6 e 7 del DPA. L'art. 6 prevede che il padrone d'azienda, il datore di lavoro, il mandante o la persona rappresentata risponda penalmente per l'autore che agisce intenzionalmente o per negligenza (subordinato, mandatario o rappresentante) nel caso in cui ometta di impedire un'infrazione, ovvero di paralizzarne gli effetti intenzionalmente o per negligenza. Se il datore di lavoro è una persona giuridica, una società in nome collettivo o in accomandita, una ditta individuale o una comunità di persone senza personalità giuridica, quanto sopra detto si applica agli organi, ai membri degli organi, ai soci preposti alla gestione, alle persone effettivamente dirigenti o ai liquidatori colpevoli. L'Art. 7 del DPA precisa poi che l'autorità possa condannare l'azienda al pagamento della multa se inferiore ai 50.000 CHF e se la determinazione delle persone punibili comporta, rispetto alla pena, provvedimenti d'inchiesta sproporzionati.

Vi sono particolari aspetti legali connessi all'uso di tecnologie quali sito Web, Blockchain?
L'uso di nuove tecno- *segue a pag. 2→*

All'interno:

segue da pag. 1→

La nuova Legge sulla Protezione dei Dati (nLPD)

logie deve essere attentamente valutato dalle aziende proprio perché la veloce evoluzione delle tecnologie pone sfide sempre piu' complesse per la protezione dei dati. È il caso dei siti web e dei canali online dove utenti navigano fornendo numerosi dati personali (es. indirizzo IP). Per nuove tecnologie si intendono anche strumenti e sistemi, ad esempio i cookies, che permettono di tracciare il comportamento di navigazione online per creare dei profili comportamentali al fine di inviare pubblicità personalizzata anche attraverso piattaforme non proprietarie. È importante che gli utenti siano informati in maniera chiara e trasparente rispetto a questi specifici trattamenti, e che possano decidere liberamente e consapevolmente di rifiutare di essere sottoposti a tali meccanismi. Tornando al tema delle sfide per la protezione dei dati, le blockchain sicuramente presentano tre aspetti di complessa gestione: l'immodificabilità dei dati che può avvenire solo mediante coinvolgimento di tutti i blocchi gerarchicamente adeguati; la natura pubblica e consultabile dei dati personali; la conservazione illimitata. La nLPD prevede che un utente possa richiedere la modifica o la cancellazione dei dati. L'interessato, inoltre, potrebbe non aver accettato che i dati possano essere accessibili.

Cos'è la Privacy Desk Suisse?
Privacy Desk Suisse SA offre un servizio di consulenza e formazione in ambito privacy di alto livello, completo e al passo con la nuova Legge sulla Protezione dei Dati (nLPD) e con le principali normative privacy mondiali, come il GDPR.
La società vanta collaborazioni strategiche con Privacy Professional svizzeri e internazionali e, per il servizio di consulenza e formazione Privacy, si avvale di Data Protection Officer, Privacy Manager e Privacy Specialist certificati UNI 11697:2017 da CEPAS (società di Bureau Veritas Italia SpA). I Consulenti sono altresì docenti della formazione continua nei CAS in tema di privacy e data protection presso SUPSI (Scuola universitaria professionale della Svizzera italiana) – dipartimento tecnologie innovative.

IMPRESSUM
NewsletterLavoro è la pubblicazione mensile del sistema d'informazione **Il diritto del lavoro applicato**.
Editore: Boss Editore SA
Resp. Newsletter: Gian Luigi Trucco
Hanno collaborato: Roberta De Giusti, Matteo Colombo, Costantino Delogu e Simone Beraldi
Boss Editore SA - CH 6900 Lugano
tel. +41(0)91 600 93 03
Amministrazione: info@boss-editore.ch

Aspetti organizzativi ed operativi per l'azienda

Matteo Colombo (Direttore di Privacy Desk Suisse SA)

Come la nuova LPD impatta sull'organizzazione aziendale?
La nuova legge federale sulla protezione dei dati (nLPD) imporrà alle aziende private e agli organi federali della Confederazione Elvetica di mettere all'ordine del giorno dei loro Consigli di Amministrazione la previsione di investimenti economici ed organizzativi in tema di ruoli e responsabilità dei soggetti che trattano i dati, aggiornamento documentale e difesa del dato.
In termini documentali, fra l'altro, si dovrà:
- aggiornare le informative da fornire agli interessati (dipendenti, clienti, utenti);
- redigere un registro delle attività di trattamento (nei casi di non obbligatorietà è comunque altamente consigliato);
- formalizzare i contratti privacy dei servizi aziendali affidati a terzi in outsourcing (nomina a responsabile) con la predisposizione di un elenco di soggetti;
- formare e istruire gli autorizzati al trattamento;
- redigere politiche sull'utilizzo degli strumenti informatici, sulla gestione della violazione dei dati, sulla conservazione dei dati e una politica di riscontro alle richieste degli interessati;
- valutare i rischi sui singoli trattamenti presenti in azienda, conducendo un'analisi dei rischi.

La nuova legge impatterà sull'organizzazione aziendale se cambierà la cultura aziendale nell'attenzione del trattamento dei dati di dipendenti, clienti e utenti; la difesa del dato e il corretto trattamento dei dati visti come una valorizzazione degli asset aziendali: quindi non un costo ma un vero e proprio investimento.

Quali misure organizzative richiede, anche in ambito IT, per rispettare le nuove norme?
La legge e l'ordinanza federale richiedono alle aziende di trattare i dati garantendo una sicurezza adeguata, definendo la necessità di protezione dei dati personali e stabilendo i provvedimenti tecnici ed organizzativi adeguati in considerazione del rischio.
Mentre è abbastanza chiaro ed intuitivo che le misure tecniche siano legate a strumenti informatici (ad esempio antivirus, firewall, backup dei dati, log management ecc.), implementare le misure organizzative significa:
- definire e fornire ai propri collaboratori le politiche sul trattamento dati;
- definire le politiche di accesso ai dati;
- organizzare il controllo all'accesso dei locali e agli impianti (si pensi alle sale server);
- definire un organigramma privacy aziendale che individui i soggetti referenti interni ed esterni;
- investire su percorsi di formazione e sensibilizzazione in materia di trattamento dei dati e cybersicurezza;
- definire una politica sulla conservazione dei dati.

Come gestire la questione del "consenso" nel trattamento dei dati?
Il consenso è una delle basi giuridiche fondamentali per il trattamento dati nell'Unione Europea e anche all'interno della legge sulla protezione dei dati Svizzera il consenso è visto come una delle condizioni per autorizzare il Titolare del trattamento a trattare un dato soprattutto per:
- il trattamento di dati personali degno di particolare protezione;
- la profilazione a rischio elevato da parte di privati;
- la profilazione da parte di un organo federale.

Il consenso deve essere:
- informato, è necessario sottoporre l'informativa all'interessato prima ancora della raccolta dei suoi dati e l'informativa deve contenere tutte quelle informazioni che permettono all'interessato di effettuare una scelta consapevole e di comprendere perché, in che modo, dove e per quanto tempo verranno utilizzati i suoi dati;
- libero, quindi, non possiamo obbligare a fornire un consenso marketing o di profilazione per ricevere la prestazione contrattuale;
- specifico, non possiamo chiedere un unico consenso per più finalità (es. marketing, profilazione e cessione dati terzi), ma dovremo chiedere più consensi liberi sulle singole finalità;
- facilmente revocabile, in modo semplice da parte dell'interessato, come è stato semplice raccoglierlo dovrà essere facilmente revocato;
- verificabile, soprattutto nei servizi offerti via web - ad esempio attraverso sistemi di "*doppio opt in*" - per provare anche origine ed esattezza del dato.

E per gli eventuali servizi aziendali affidati a terzi in outsourcing?
La verifica dei soggetti esterni che trattano il dato in nome e per conto del Titolare del trattamento è uno degli aspetti fondamentali per la corretta gestione del trattamento dati. Da anni le aziende esternalizzano il trattamento dati di molte attività interne. Pensiamo, ad esempio, all'elaborazione buste paga effettuata spesso da consulenti esterni che utilizzano sistemi informatici on-premise o Cloud di altre società esterne: quindi un trattamento aziendale che vede addirittura una catena di soggetti esterni che intervengono sui dati del Titolare del trattamento. Pertanto, i Titolari del trattamento dovranno formalizzare i contratti anche da un punto di vista privacy e di sicurezza del dato e dovranno anche

verificare che questi fornitori terzi siano qualificati ed adeguati da un punto di vista di misure di sicurezza tecniche e organizzative, onde evitare responsabilità in caso di trattamento illecito o di violazione di dati.

Esistono integrazioni fra nLPD e certificazioni/sistemi ISO?

La nuova legge federale sulla protezione dei dati contempla la possibilità per le aziende di adottare codici di condotta, ovvero prevede che le associazioni professionali di settore ed economiche, autorizzate dai loro statuti, possano sottoporre codici di condotta all'Incaricato Federale della protezione dei dati (IFPDT); inoltre potranno anche esserci aziende che avranno la facoltà di sottoporre i loro sistemi ad una valutazione da parte di organismi di certificazione previo riconoscimento di queste certificazioni da parte dell'IFPDT.

A livello internazionale è attualmente attiva la norma ISO/IEC 27701 che specifica i requisiti e fornisce indicazioni per implementare, attuare, mantenere e migliorare costantemente un sistema di gestione delle informazioni sulla privacy (PIMS); la norma si basa sui requisiti della norma ISO/IEC 27001, lo standard per i sistemi di gestione della sicurezza delle informazioni (ISMS) e sul Codice di buone pratiche per i controlli della sicurezza delle informazioni nella ISO/IEC 27002.

Quando è necessario il DPO e quale è il suo ruolo?

La norma svizzera non prevede l'obbligo, ma solo la facoltà, per le aziende private di individuazione e nomina di un Data Protection Officer, conosciuto in Svizzera come Consulente per la protezione dei dati. Il ruolo del DPO deve essere un ruolo di facilitatore ed interlocutore per:

- le persone interessate (dipendenti, clienti o utenti di servizi);
- l'Autorità Garante privacy (IFPDT);
- il Management ed il Titolare del trattamento.

Il DPO è quindi una figura chiave all'interno dell'organizzazione e fra i suoi compiti vi è quello di fornire formazione e consulenza al Titolare del trattamento, partecipare all'applicazione della protezione dei dati, nonché fornire suggerimenti rispetto alle misure tecniche ed organizzative che il Titolare ha posto in essere o dovrebbe attuare.

Meglio un DPO interno o esterno?

In Svizzera troviamo entrambe le situazioni; alcuni Titolari del trattamento preferiscono organizzarsi con un Data Protection Officer interno che probabilmente ha come vantaggio una migliore conoscenza del settore ed una maggiore facilità di confronto con le figure interne; di contro si dovrà analizzare il tema di eventuale conflitto di interessi nei casi in cui l'attività da DPO non sia l'unica all'interno dell'organizzazione.

Altre aziende preferiscono invece scegliere DPO esterni perché hanno una maggiore conoscenza della normativa e delle prassi operative delle Autorità Garanti Privacy, inoltre hanno un team di esperti in tema di data protection, cybersicurezza e conoscenza dei processi di trattamento.

Quali sanzioni sono previste dalla nuova LPD?

La nuova legge sulla protezione prevede una sanzione penale per i privati, a querela di parte, con multa fino a 250.000 CHF; oppure sempre fino a 250.000 CHF per tutti quei privati che

intenzionalmente non ottempereranno ad una decisione dell'IFPDT. La norma prevede altresì la possibilità di sanzionare direttamente l'azienda, se la multa non supera i 50.000 CHF, quando non si è in grado, se non con sforzo sproporzionato, di determinare le persone punibili. Un effetto da non sottovalutare è anche la possibilità da parte dell'IFPDT di pubblicare nel rapporto annuale il nome dell'azienda sanzionata, riportando quindi nei confronti dell'azienda un danno reputazionale non trascurabile.

Il Regolamento Europeo sulla Protezione dei dati GDPR si applica alle aziende svizzere?

Anche alle aziende che non hanno sede in Europa si può applicare la norma privacy europea; infatti, il GDPR è applicabile per le aziende svizzere qualora trattino dati di cittadini europei al fine di offrire beni o prestare servizi nell'Unione, oppure in caso di monitoraggio del loro comportamento nella misura in cui tale comportamento abbia luogo all'interno dell'Unione. Facciamo un esempio: se un'azienda svizzera ha un sito web dove permette di acquistare beni o servizi dall'Europa, se vi sono alcuni elementi presenti nel sito, si applicherà il Regolamento Europeo sulla protezione dei dati; da qui l'obbligo di inserire, ad esempio, un'informativa non solo LPD ma anche GDPR.

Quali sono quindi in concreto i casi in cui ad un sito web Svizzero si applica il GDPR?

Quando all'interno del sito web sono presenti alcuni dei seguenti elementi:

- l'UE, o almeno uno Stato membro, sono indicati nominativamente in riferimento al bene o al servizio offerto;
- il Titolare o il Responsabile del trattamento paga il gestore di un motore di ricerca per un servizio di posizionamento su Internet al fine di facilitare l'accesso al proprio sito da parte dei consumatori dell'Unione;
- il Titolare o il Responsabile del trattamento ha avviato campagne pubblicitarie e di marketing rivolte al pubblico di un paese dell'UE;
- la natura internazionale dell'attività in questione, come ad esempio certe attività turistiche;
- la menzione di indirizzi o numeri di telefono appositi da utilizzare da un Paese dell'UE;
- l'uso di un nome di dominio di primo livello diverso da quello del Paese terzo in cui il Titolare o il Responsabile del trattamento è stabilito, ad esempio «.de», oppure l'uso di nomi di dominio di primo livello neutri, ad esempio «.eu»;
- la descrizione delle istruzioni di viaggio da uno o più Stati membri dell'UE verso il luogo in cui viene fornito il servizio;
- la menzione di una clientela internazionale composta di clienti domiciliati in vari Stati membri dell'UE, in particolare mediante la presentazione di scritture contabili redatte da tali clienti;
- l'uso di una lingua o di una valuta diversa da quelle generalmente utilizzate nel Paese del commerciante, in particolare una lingua o una valuta di uno o più Stati membri dell'UE;
- il Titolare del trattamento dei dati offre la consegna di beni negli Stati membri dell'UE.

Quando entrerà in vigore la nLPD per le aziende del settore privato svizzero?

La nuova legge federale sulla protezione dei dati (nLPD) e l'Ordinanza sulla protezione dei dati (OPDA) entreranno in vigore il 1° settembre 2023.

MATTEO COLOMBO – *Presidente*
Dottore in Giurisprudenza. Direttore di Privacy Desk Suisse SA, CEO di Labor Project srl e Presidente di ASSO DPO | Associazione Data Protection Officer. Docente presso la SUPSI per il CAS GDPR - nLPD. Consulente e formatore in materia di Privacy e compliance dal 2003. Ha conseguito certificazioni internazionali per competenze privacy quali: Certified Information Privacy Professional Europe (CIPP/E), Certified Information Privacy Manager (CIPM) e Fellow of Information Privacy (FIP) rilasciate da IAPP. Ha conseguito altresì la certificazione CEPAS UNI 11697 come Data Protection Officer (DPO). DPO advisor di alcune multinazionali in Svizzera e in Europa. Relatore in molteplici eventi in Italia e in Svizzera sui temi Privacy e D.Lgs. 231/01, docente nei corsi CAS GDPR e Master in ICT System, Security e Cybercrime presso SUPSI e autore di diversi libri sul Regolamento (UE) Privacy.

ROBERTA DE GIUSTI – *Country Manager*
Dottoressa in Servizi Giuridici per giuristi d'impresa. Formatrice ed esperta in materia di Privacy. Data Protection Officer (DPO). Ha conseguito la certificazione CEPAS UNI 11697 come Data Protection Officer (DPO) ed è Valutatore interno ISO 27001 qualificato da Bureau Veritas Italia SpA. Componente di Team DPO advisor di alcune multinazionali in Svizzera. Docente presso l'università SUPSI (Scuola Universitaria Professionale della Svizzera Italiana).