economiesuisse

Protezione dei dati: panoramica della nuova legge

La revisione della legge svizzera sulla protezione dei dati (LPD) è conclusa. Le nuove regole e le disposizioni d'applicazione contenute nella nuova ordinanza sulla protezione dei dati (OPDa) e la nuova ordinanza sulle certificazioni in materia di protezione dei dati (OCPD) entrano in vigore il 1° settembre 2023. Non è previsto nessun periodo di transizione.

Si raccomanda alle imprese svizzere di familiarizzare il più rapidamente possibile con la nuova legge e le sue esigenze e di adattare il loro dispositivo di protezione dei dati, in particolare le loro disposizioni relative alla protezione dei dati e i contratti. economiesuisse risponde alle questioni più urgenti in collaborazione con due avvocati, Cornelia Stengel e Luca Stäuble, alfine di segnalare alle imprese svizzere le misure da adottare in relazione all'entrata in vigore della nuova legge sulla protezione dei dati.

L'unico scopo di questa panoramica è fornire informazioni e sensibilizzare l'opinione pubblica. Tuttavia, non sostituisce la consulenza legale ed economiesuisse non può essere ritenuta responsabile di eventuali azioni od omissioni derivanti dalla lettura di questo contributo.

Media-Link:
https://www.youtube.com/watch?v=EImPV2xNtDE

FAQ

1) Quali sono lo scopo e il campo d'applicazione della nuova legge (nLPD)?

La nuova legge (nLPD) mira a proteggere la personalità e i diritti fondamentali delle persone fisiche residenti in Svizzera i cui dati sono trattati da privati (società private) o dallo Stato. I dati delle persone giuridiche non saranno più protetti. L'idea di fondo è quella di offrire alle persone interessate una maggiore trasparenza e quindi di rafforzare i loro diritti sui propri dati ("autodeterminazione informativa"). La nuova legge mira anche a promuovere misure preventive e la responsabilità individuale dei responsabili del trattamento dei dati. A tal fine, la legge rafforza il monitoraggio della protezione dei dati e amplia le disposizioni di diritto penale. Introduce inoltre nuovi obblighi per le imprese, in particolare in caso di raccolta, perdita o uso improprio dei dati personali.

2) Perché era necessaria una revisione della legge attuale?

L'attuale legge svizzera sulla protezione dei dati risale al 1992. Da allora, con il passaggio alla digitalizzazione da parte dell'economia e della società, la raccolta e l'utilizzo dei dati personali si sono ampliati. A livello globale, e in particolare all'interno dell'UE, la protezione dei dati è stata notevolmente rafforzata e le organizzazioni internazionali hanno inasprito gli standard minimi in questo settore. Per la Svizzera è stato quindi necessario adattare la legge del 1992 alle nuove abitudini dei consumatori (acquisti online, social network, ecc.), agli sviluppi tecnologici (digitalizzazione, intelligenza artificiale, ecc.) e agli standard internazionali.

Con l'adozione del Regolamento generale sulla protezione dei dati (GDPR), l'Unione europea ha stabilito un nuovo standard su scala internazionale. Questo regolamento, entrato in vigore il 25 maggio 2018, sta facendo scalpore in tutto il mondo per la sua portata extraterritoriale. Molte imprese svizzere rientrano nell'ambito di applicazione del GDPR, in quanto si concentrano sui mercati dell'UE o dello SEE. Inoltre, il GDPR prevede che i dati personali possano essere trasferiti a un paese terzo solo se tale paese ha un livello di protezione dei dati «adeguato» dal punto di vista dell'UE. Un flusso di dati senza problemi dall'UE è particolarmente importante per paesi come la Svizzera, che hanno legami economici molto stretti con l'UE.

Un obiettivo importante della revisione della LPD era quindi quello di sviluppare una soluzione coordinata a livello internazionale - «equivalente» agli occhi dell'UE - che incoraggiasse gli sviluppi tecnologici nell'economia dei dati e, allo stesso tempo, non abbandonasse i punti di forza della legislazione attuale.

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

La Svizzera è un «paese terzo» dal punto di vista dell'UE. Per trasferire i dati a un paese terzo, la Commissione europea deve emettere una decisione sull'adeguatezza del sistema svizzero. La Svizzera dispone di tale decisione, ma si basa sulla vecchia legislazione europea. Ma con la revisione della LPD, la Svizzera dovrebbe aver creato le condizioni necessarie affinché la Commissione europea continui a classificare la legge svizzera sulla protezione dei dati (rivista) come adeguata. La (nuova) decisione sull'adeguatezza è attualmente in sospeso.

Non da ultimo non va dimenticato che la modernizzazione del diritto svizzero avviene in un contesto internazionale in cui i cittadini e i consumatori di tutto il mondo chiedono una migliore protezione dei loro dati personali e un maggiore controllo su di essi. Questa tendenza è riscontrabile non solo nell'UE, ma in molti paesi, tra cui la Nuova Zelanda. La California ha inasprito la propria legislazione sulla protezione dei dati, basandosi in parte sugli standard dell'UE.

3) Dove si applica la nuova legge?

Sebbene la nLPD si applichi sul territorio svizzero, ha anche una portata extraterritoriale (principio degli effetti), in quanto si applica a stati di cose che si verificano all'estero e producono effetti in Svizzera (art. 3). In altre parole, se il trattamento dei dati personali avviene al di fuori della Svizzera, ma riguarda persone fisiche stabilite in Svizzera e produce effetti in Svizzera, il titolare del trattamento in questione è tenuto a rispettare la direttiva nLPD. A determinate condizioni, il titolare del trattamento deve anche nominare un rappresentante legale in Svizzera (artt. 14 e 15 nLPD).

Esempio: una società con sede all'estero tratta i dati di persone fisiche residenti in Svizzera dall'estero. In questo caso, ogni situazione deve essere valutata individualmente. La nLPD si applica a prescindere dal fatto che il trattamento dei dati sia o meno «sensibile» in Svizzera - questo dovrebbe essere già il caso, come regola generale, quando i dati sono trattati per un certo numero di persone in Svizzera. Il GDPR, invece, si basa - a condizione che non vi sia una sede nell'UE - sul fatto che il trattamento dei dati sia legato all'orientamento «manifestamente intenzionale» dell'offerta di beni o servizi verso persone nell'UE (ad esempio l'online shop è orientato in questa direzione) o all'osservazione del comportamento in relazione a persone nell'UE (ad esempio l'uso di tecnologie di web-tracking). La portata geografica della nuova regolamentazione svizzera è quindi ancora più ampia di quella del GDPR.

4) Quando entra in vigore la nuova legge (nLPD)?

Il 31 agosto 2022 il Consiglio federale ha pubblicato l'Ordinanza sulla protezione dei dati (OPDa) e ha stabilito che le nuove regole entreranno in vigore il 1° settembre 2023. Dato che la legge non prevede un periodo di transizione, questo è un buon momento per valutare l'implementazione delle modifiche necessarie.

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

La nuova LPD si basa sul GDPR, ma presenta una serie di caratteristiche particolari. Nella maggior parte dei casi, la legge svizzera è meno formalista e presenta meno requisiti rispetto al GDPR. Ad esempio, rimane valido il principio secondo cui il trattamento dei dati personali è autorizzato nella misura in cui sono rispettati i suoi principi (art. 6 nLPD). A differenza dell'UE, non è quindi necessario avere una giustificazione (art. 6 GDPR) per trattare i dati personali.

Su alcuni punti, però, la nuova legge svizzera sarà più severa del GDPR. Si tratta dell'ambito geografico (cfr. punto 3) e dell'ambito materiale (art. 2 nLPD). Secondo la nLPD, quest'ultimo copre tutti i trattamenti dei dati (automatizzati e manuali),

mentre il GDPR si applica solo ai sistemi di file per quanto riguarda il trattamento manuale dei dati. In seguito, l'obbligo di fornire informazioni sulla raccolta di dati personali ai sensi della direttiva nLPD va oltre il GDPR, in quanto, in caso di trasmissione di dati all'estero, devono essere fornite informazioni su tutti gli Stati destinatari (art. 19 della direttiva nLPD). La nLPD prevede inoltre l'obbligo di registrare il trattamento automatizzato dei dati e di redigere un regolamento per il trattamento automatizzato (artt. 4 e 5 e segg. OPDa). Inoltre, in base all'ordinanza della nLPD - a differenza del GDPR, che prevede multe esclusivamente per le imprese - le sanzioni si applicano alle persone fisiche (art. 60 e segg. nLPD) e, infine, il concetto di «dati personali sensibili» comprende due ulteriori categorie: procedimenti e sanzioni amministrative o penali e misure di assistenza sociale.

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

No. Tutte le imprese, senza eccezioni, sono interessate dalla nuova LPD. Indipendentemente dalle sue dimensioni, un'impresa possiede una grande quantità di dati su clienti, partner, fornitori e collaboratori. Con la digitalizzazione dell'economia, la quantità di dati personali trattati dalle imprese, comprese le PMI, continuerà a crescere. Tuttavia, alcuni dei (nuovi) obblighi previsti dalla nLPD dipendono dalla portata del trattamento dei dati e dal rischio che il trattamento comporta per la personalità o i diritti fondamentali degli interessati. Questo approccio basato sul rischio, che si applica tra l'altro alla sicurezza dei dati, significa che le misure possono essere adottate caso per caso. È ovvio che anche le PMI possono trattare dati personali sensibili su larga scala o svolgere altre attività di trattamento che comportano un rischio elevato per la personalità degli interessati.

Tutte le imprese, comprese le PMI, devono prepararsi adeguatamente all'entrata in vigore della nuova legge. Poiché la legge è allineata agli standard europei, ciò è particolarmente vero per le imprese svizzere che non hanno ancora adattato i loro sistemi di protezione dei dati al GDPR.

L'unica «eccezione per le PMI» riguarda l'obbligo di tenere un registro delle attività di trattamento. Le PMI con meno di 250 dipendenti al 1° gennaio sono esenti da tale obbligo, a condizione che non trattino «dati personali sensibili» su larga scala e non effettuino «profiling ad alto rischio». È comunque nell'interesse di un'azienda tenere tale registro delle attività di trattamento su base volontaria, in quanto può fornire una preziosa panoramica del trattamento dei dati effettuato all'interno dell'impresa e quindi servire come base per adempiere ad altri obblighi, come gli obblighi di informazione nei confronti degli interessati.

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

La nuova legge introduce nuovi obblighi. I principali sono:

- l'obbligo di mettere in atto misure tecniche e organizzative per garantire che il trattamento dei dati sia conforme ai requisiti di protezione dei dati fin dall'inizio e per impostazione predefinita, in particolare per garantire che i principi stabiliti per il trattamento siano rispettati e che il trattamento sia limitato al minimo necessario per raggiungere lo scopo previsto (art. 7

nLPD) (si vedano i nuovi termini al successivo punto 12);

- l'obbligo di cancellare (o rendere anonimi) i dati personali che non sono più necessari per il raggiungimento degli obiettivi perseguiti e che non sono soggetti a un obbligo legale di conservazione è già in vigore in virtù del principio di proporzionalità ed è ora esplicitamente sancito dalla legge (art. 6, par. 4, nLPD);

- l'obbligo di istituire e mantenere un registro delle attività di trattamento dei dati. Le imprese con meno di 250 dipendenti beneficiano di un'eccezione se il trattamento dei dati comporta un basso rischio di danno alla personalità degli interessati (art. 12 nLPD e punto 6 del presente documento). L'OPDa specifica che il rischio è elevato quando i dati personali sensibili sono trattati su larga scala o quando viene effettuata una profilazione ad alto rischio (art. 24);

- l'obbligo di notifica all'Incaricato federale della protezione dei dati e delle informazioni (IFPDT) e alla persona interessata in caso di violazione della sicurezza dei dati (art. 24 nLPD e art. 15 dell'OPDa). A differenza del GDPR (che fissa un termine di 72 ore per la notifica), la nLPD non fissa un termine esplicito, ma stabilisce che la notifica deve essere effettuata «il più presto possibile». Il contenuto obbligatorio e la documentazione sono disciplinati dall'OPDa (art. 15);

- l'obbligo di effettuare una valutazione preventiva dell'impatto sulla protezione dei dati quando il trattamento dei dati comporta un rischio elevato per la personalità o i diritti fondamentali dell'individuo (art. 22 nLPD e art. 14 OPDa);

- l'obbligo di fornire informazioni al momento della raccolta dei dati personali, sia che questi vengano raccolti direttamente dall'interessato che da terzi (art. 19 e segg. nLPD e art. 13 OPDa). Va notato che le informazioni relative alla raccolta dei dati personali devono essere semplici e comprensibili per le persone interessate. Questo aspetto deve essere tenuto in considerazione, in particolare nella stesura delle disposizioni sulla protezione dei dati. Per quanto riguarda l'obbligo di fornire informazioni, la nLPD è più severa del GDPR e questa è un'eccezione (si veda anche il punto 5). Una violazione (eventualmente) intenzionale di questo obbligo è punibile penalmente;

- l'obbligo di informare in caso di decisione individuale automatizzata, ossia una decisione basata esclusivamente su un trattamento automatizzato e che comporti conseguenze giuridiche per l'interessato o che lo riguardi in modo significativo (art. 21 nLPD). Una violazione (eventualmente)

intenzionale di questo obbligo è punibile penalmente;

- l'obbligo di registrare i trattamenti automatizzati su larga scala di dati personali sensibili o di profiling ad alto rischio qualora le misure preventive adottate non garantiscano la protezione dei dati (art. 4 OPDa) e di redigere regole per tali trattamenti automatizzati e di aggiornarle regolarmente (art. 5 OPDa).

8) Quali sono i nuovi diritti delle persone interessate?

L'obiettivo principale della nuova normativa è quello di migliorare la trasparenza e la protezione dei dati personali degli interessati. A tal fine, le imprese devono fornire informazioni sulla raccolta dei dati personali in modo conciso, comprensibile e facilmente accessibile (art. 13 OPDa) e i diritti delle persone devono essere rafforzati. I diritti individuali includono, ad esempio:

- il diritto di essere informato sul trattamento dei propri dati personali (art. 25-27 nLPD);
- il diritto alla consegna o alla trasmissione dei dati personali (portabilità dei dati) (artt. 28 e 29 nLPD);
- il diritto di non essere oggetto di una decisione individuale automatizzata (art. 21 nLPD).

Alcune violazioni (potenzialmente) intenzionali dell'obbligo di informazione sono punibili (art. 60 nLPD). Le imprese devono quindi assicurarsi di avere sempre una visione d'insieme dei dati personali che trattano e di essere in grado di rispondere alle richieste degli interessati nei tempi e nelle forme previste.

9) Ho bisogno dell'autorizzazione dell'interessato per trattare i dati delle persone interessate?

No. Il trattamento dei dati personali è consentito sia dalla legge vigente che da quella nuova, a condizione che non vi sia una violazione illegale della privacy degli interessati. Una violazione della privacy si verifica in particolare quando:

- il trattamento dei dati personali non rispetta i principi del trattamento dei dati (art. 6 nLPD) e della sicurezza dei dati (art. 8 nLPD);
- alcuni dati personali sono trattati contrariamente alla dichiarazione di volontà espressa dalla persona interessata;
- alcuni dati personali sensibili sono comunicati a terzi.

A differenza del GDPR, in linea di principio non è richiesta una giustificazione (si veda anche il punto 5). Pertanto, ai sensi della nLPD, continua ad applicarsi il «principio dell'autorizzazione con riserva di obiezione», mentre secondo il GDPR si applica il «divieto di principio con riserva di autorizzazione» (artt. 6 e 9 GDPR).

10) Cosa devo tenere presente quando utilizzo operatori esterni che trattano dati personali per nostro conto (fornitori di servizi cloud, fornitori di servizi HR, ecc.)?

Gli operatori esterni che trattano dati personali per conto e su istruzioni del committente o del «responsabile del trattamento» (si veda il successivo punto 12), come i fornitori di servizi cloud, gli host web, i servizi di gestione dei salari, ecc. sono considerati «incaricati del trattamento» (art. 5, lett. k nLPD).

Il trattamento dei dati personali può - come avviene già oggi - essere affidato per contratto o per legge a un incaricato del trattamento, se l'incaricato del trattamento tratta i dati come sarebbe autorizzato a fare il responsabile del trattamento e se nessun obbligo legale o contrattuale di mantenere la segretezza vieta la delega (art. 9 nLPD). Il ricorso a un incaricato del trattamento presuppone quindi in genere un contratto scritto (accordo per il trattamento dei dati da parte di un incaricato o CTD). Prima della delega, il committente o il responsabile deve assicurarsi che l'incaricato del trattamento sia in grado di garantire la sicurezza dei dati (art. 8 nLPD e art. 1 e segg. OPDa). L'incaricato del trattamento è obbligato per legge a ottenere un'autorizzazione preventiva (generale o specifica) dal responsabile del trattamento prima di ricorrere a un terzo per il trattamento dei dati (art. 7 OPDa). Le parti possono includere altri punti nel CTD (ad esempio, la procedura da seguire in caso di reclamo da parte degli interessati o di violazione della sicurezza dei dati, i diritti di verifica e controllo, la responsabilità, il foro competente, ecc. In pratica, vengono comunemente utilizzati contratti-modello basati sul contenuto minimo secondo il GDPR.

Il fatto di affidare intenzionalmente il trattamento dei dati ad un subappaltatore mentre le condizioni previste dall'art. 9 cpv. 1 e 2 non sono soddisfatte è punibile (art. 61 lett. b nLPD).

11) Posso comunicare o trasmettere dati personali all'estero?

Per divulgazione di dati personali si intende «la trasmissione o la messa a disposizione di dati personali» (art. 5 lett. b nLPD). Pertanto, anche la semplice possibilità di accesso ai dati da parte di un'organizzazione all'estero (ad esempio, un team di assistenza) costituisce una divulgazione ai sensi della nLPD.

La comunicazione di dati personali all'estero è autorizzata a condizione che lo Stato destinatario disponga di una legislazione che garantisca un livello «adeguato» di protezione dei dati (art. 16 cpv. 1 nLPD). Gli Stati che soddisfano questa condizione sono definiti dal Consiglio federale e pubblicati nell'Allegato 1 dell'Ordinanza sulla protezione dei dati.

Per contro, ciò significa che tutti gli Stati che non figurano su questa lista non dispongono di un livello di protezione dei dati «adeguato» e che quindi i dati personali possono essere comunicati solo se vengono adottate misure di protezione aggiuntive (art. 16, cpv. 2 e art. 17 nLPD nonché art. 9 OPDa). A tal fine si utilizzano le clausole contrattuali standard di protezione dei dati (SCC). L'esportatore di dati deve adottare misure adeguate per garantire che il destinatario dei dati rispetti le SCC (art. 10 OPDa). Dato che le SCC sono vincolanti solo per il destinatario in quanto parte contraente, ma non per le autorità locali, e che i dati personali trasferiti non sono quindi protetti dall'accesso da parte di uno Stato, l'esportatore di dati deve innanzitutto valutare il rischio di accesso ai dati da parte delle autorità dal punto di vista svizzero, effettuando un «Transfer Risk Assessment» (TIA) (clausola 14 SCC). A seconda del rischio, è necessario adottare

ulteriori misure di protezione (ad esempio, pseudonimizzazione, crittografia dei dati) o non trasferire i dati.

La violazione (potenzialmente) intenzionale delle disposizioni relative alla comunicazione di dati personali all'estero è soggetta a sanzioni (art. 61, lett. a nLPD).

Per quanto concerne la comunicazione di dati personali agli Stati Uniti, vorremmo richiamare l'attenzione sul nuovo Data Privacy Framework (DPF) UE-USA, che consente alle aziende statunitensi di essere certificate come importatori di dati. Dalla decisione di adeguatezza della Commissione europea del 10 luglio 2023, i trasferimenti di dati dall'UE a società statunitensi certificate ai sensi del Data Privacy Framework sono considerati trasferimenti di dati verso un paese che offre un livello «adeguato» di protezione dei dati (si veda il link al comunicato stampa). Si prevede che l'IFPDT stabilirà a breve il livello di protezione per la Svizzera (CH-US Data Privacy Framework) per i trasferimenti di dati nell'ambito di questo quadro.

12) Quali nuovi termini sono importanti per comprendere il diritto della protezione dei dati?

La nuova legge sulla protezione dei dati ha introdotto alcuni nuovi termini o li ha parzialmente armonizzati con il GDPR. I principali sono:

- I dati personali: Il termine si applica solo alle persone fisiche. I dati relativi alle persone giuridiche non sono dunque interessati e sono pertanto esclusi dal campo di protezione della LPD (art. 1 e art. 5, let. a nLPD).
- I dati personali sensibili: Sono ora anche interessati i dati relativi all'appartenenza ad un'etnia, i dati genetici e i dati biometrici (che permettono un'identificazione univoca) (art. 5, let. c nLPD).
- Responsabile del trattamento: Corrisponde al «detentore di una collezione di dati» ai sensi della legge vigente e al «responsabile del trattamento dei dati» ai sensi del GDPR. Si tratta di un privato (in particolare un'azienda) o di un ente federale che, da solo o insieme ad altri, decide le finalità e i mezzi del trattamento dei dati personali (art. 5, lett. j nLPD). Ad esempio, un datore di lavoro che tratta i dati personali dei propri dipendenti nell'ambito dell'esecuzione del contratto di lavoro o un rivenditore che tratta i dati personali dei propri clienti nell'ambito dell'esecuzione del contratto di vendita.
- Incaricato del trattamento: Un incaricato del trattamento è una persona che tratta dati personali per conto del titolare del trattamento, ad esempio i fornitori di servizi cloud (art. 5 let. k nLPD, cfr. punto 10 sopra).
- Profiling: Questo termine si riferisce a qualsiasi forma di trattamento automatizzato di dati personali che implica l'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica (in particolare per analizzare o prevedere fattori quali il rendimento lavorativo, la situazione economica, la salute, le preferenze personali, gli interessi e il luogo di soggiorno). Conseguenze giuridiche più gravi si applicano però solo alla «profilazione ad alto rischio», che comporta un rischio marcato per la personalità o i diritti fondamentali della persona interessata, perché porta a una corrispondenza di dati che consente di valutare le caratteristiche personali essenziali di una persona fisica. La profilazione ad

alto rischio è paragonabile all'attuale concetto di «profilo della personalità». Va notato che la nLPD non introduce un requisito di consenso per la profilazione ad alto rischio, ma si limita a richiedere che il consenso, se dovesse essere richiesto come giustificazione ai sensi dell'art. 31 nLPD, sia «esplicito». In questo contesto, va ricordato che il trattamento dei dati personali non richiede in linea di principio alcuna giustificazione, né ai sensi della legge esistente né ai sensi della nuova legge (cfr. punti 5 e 9).

- Principi di «Privacy by Design» e di «Privacy by Default»: La nLPD introduce i principi di «Privacy by Design» e «Privacy by Default». Come suggerisce il nome, il principio della «Privacy by Design» significa che devono essere adottate misure tecniche e organizzative fin dalla progettazione di un sistema di trattamento, in particolare per garantire la sicurezza dei dati personali. Il principio della «Privacy by Default» significa che le impostazioni predefinite di un sistema di elaborazione dati devono essere configurate in modo tale da trattare solo i dati personali effettivamente necessari per lo scopo di elaborazione specificato. Questa disposizione mira a proteggere gli utenti non tecnici che non sanno come modificare le impostazioni di protezione dei dati in base alle proprie preferenze. Va notato che è necessario effettuare impostazioni preliminari favorevoli alla protezione dei dati solo nei casi in cui le impostazioni possono essere modificate.

13) Quali sono i rischi di una mancata conformità alla nuova legge?

In caso di violazione della nuova legge, potreste essere passibili di sanzioni pecuniarie fino a 250'000 franchi svizzeri (se ad esempio non rispettate i vostri obblighi di informazione - artt. 19 e segg. e 25 e segg. nLPD) o del vostro dovere di diligenza, ad esempio trasferendo illegalmente dati personali all'estero (art. 16 f. nLPD) o a un incaricato del trattamento (art. 9 nLPD) o se non rispettate i requisiti minimi di sicurezza dei dati (art. 8 nLPD in relazione con l'art. 1 f. OPDa). A differenza del GDPR, le sanzioni previste dalla nLPD non sono dirette contro l'impresa che commette l'infrazione, ma contro la persona responsabile del rispetto della protezione dei dati (il direttore o il membro del consiglio di amministrazione, ma anche, in determinate circostanze, altri dipendenti). Solo il comportamento (potenzialmente) intenzionale è punibile (art. 60 e segg. nLPD). In via eccezionale, anche le imprese possono essere direttamente coinvolte se è prevista una multa fino a 50'000 franchi svizzeri e se l'identificazione del colpevole all'interno dell'azienda o dell'organizzazione comporterebbe costi di indagine sproporzionati (art. 64, cpv. 2 nLPD).

Ignorare la (nuova) legge sulla protezione dei dati può avere conseguenze non solo per il responsabile all'interno di un'impresa, ma anche per l'impresa stessa, e in particolare per la sua reputazione. Anche i poteri dell'Incaricato federale della protezione dei dati (IFPDT) sono stati ampliati (art. 51 nLPD). Ora può non solo emettere raccomandazioni, ma anche ordinare misure amministrative (ad esempio ordinare l'adeguamento, l'interruzione o la cancellazione del trattamento o la cancellazione dei dati personali), che possono essere una misura drastica per alcune aziende.

14) Come prepararsi ai cambiamenti?

Il primo passo è prepararsi il prima possibile, effettuando un'analisi delle lacune per adattare gradualmente la conformità alla protezione dei dati a questo nuovo regime normativo. A seconda delle dimensioni dell'impresa e dell'entità del trattamento dei dati, questo processo può richiedere pochi giorni o diversi mesi. Per le imprese già conformi al GDPR, il compito sarà ovviamente più semplice rispetto a quelle che sono ancora agli inizi. È comunque opportuno adottare soluzioni pragmatiche, ossia iniziare a implementare i requisiti minimi della legge (registro, obbligo di informazione, contratti con i subappaltatori, trasferimenti di dati verso paesi terzi, ecc.).

Un piano d'azione dovrebbe basarsi sui seguenti tre pilastri: sicurezza informatica, aspetti legali e governance dei dati. Su quest'ultimo punto, economiesuisse ha redatto una Carta dell'economia svizzera per una gestione responsabile dei dati. Qualora necessario, a causa della mancanza di competenze e/o di risorse interne, le imprese dovrebbero ricorrere ai servizi di esperti di sicurezza informatica e di protezione dei dati, sia per redigere o effettuare controlli a campione su documenti (ad esempio, dichiarazioni sulla protezione dei dati) o contratti (CTD), sia per elaborare programmi dettagliati di conformità (ad esempio, direttive, processi).

15) Cosa si deve fare per conformarsi? Quali azioni sono richieste?

Senza entrare nel dettaglio degli aspetti tecnici, legali e informatici della conformità alla nLPD, un piano d'azione pragmatico dovrebbe includere almeno le seguenti misure:

1. **Definire le responsabilità e le funzioni**
   Per quanto riguarda la pianificazione, è importante iniziare con la definizione delle responsabilità e l'assegnazione delle funzioni. È opportuno istituire un dipartimento centrale per la protezione dei dati (coordinatore, persona di contatto).

   In questo contesto, è possibile verificare rapidamente se è necessario nominare un consulente per la protezione dei dati (a differenza del GDPR, la nLPD prevede che ciò sia facoltativo per i privati - solo gli organi federali sono obbligati per legge a farlo, art. 10 nLPD e art. 23 OPDa).

2. **Un inventario globale è essenziale**
   Le imprese devono essere in grado di rispondere in qualsiasi momento a qualsiasi richiesta di informazioni, vale a dire che, in caso di raccolta di dati personali, devono fornire informazioni sull'identità del titolare del trattamento, sulle finalità del trattamento, sugli eventuali destinatari dei dati, ecc. Devono inoltre essere in grado di rispettare i diritti degli interessati, al fine di fornire loro informazioni sul trattamento dei loro dati personali (art. 25 e segg. nLPD e art. 16 e segg. OPDa). Ciò presuppone che le imprese sappiano quali dati personali vengono trattati e per quali finalità, se questi dati vengono comunicati ad altri paesi e ad altre persone, e così via.

   Le imprese devono quindi iniziare a fare il punto su tutti i dati che trattano. Il nuovo registro obbligatorio (il cosiddetto registro delle attività di

trattamento) può servire come punto di partenza. Ciò non solo creerà una buona base per la stesura di altri documenti (obbligatori) sulla protezione dei dati (disposizioni sulla protezione dei dati, subappalto, ecc.), ma consentirà alle imprese di dar seguito al (possibile) obbligo di tenere un registro delle attività di trattamento. Tale registro è uno sforzo collettivo di tutti i collaboratori coinvolti nel trattamento dei dati personali.

3. **Analisi delle lacune e valutazione dei rischi**
   Il lavoro necessario per raggiungere la conformità può essere identificato e quindi documentato mediante un'analisi delle lacune (confrontando lo stato attuale con l'obiettivo da raggiungere). A questo scopo si possono utilizzare anche i registri modello delle attività di elaborazione.

   Alcuni obblighi della nLPD, come i requisiti di sicurezza dei dati, l'obbligo per le PMI di tenere un registro delle attività di trattamento o l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati, dipendono dal rischio che presenta il trattamento dei dati all'interno dell'azienda. È quindi necessaria una valutazione preventiva del rischio per determinare le misure concrete da attuare. Per garantire un'adeguata sicurezza dei dati, è necessario determinare la necessità di proteggere i dati personali e definire le misure tecniche e organizzative adeguate alla luce del rischio. I criteri per determinare la necessità di proteggere i dati personali possono basarsi sui criteri di cui all'art. 1 cpv. 2 dell'OPDa, mentre i criteri per valutare il rischio per la personalità o i diritti fondamentali della persona interessata possono basarsi sui criteri di cui all'art. 1 cpv. 3 dell'OPDa. Nella definizione delle misure tecniche e organizzative si deve tenere conto anche dello stato della tecnica e dei costi di attuazione (art. 1 cpv. 4 OPDa).

   Possono sussistere rischi maggiori e quindi requisiti più elevati in termini di conformità alle normative sulla protezione dei dati (in particolare sulla sicurezza dei dati), ad esempio quando:

   - Le imprese trattano grandi volumi di dati personali. Esempio: le imprese specializzate nelle vendite online o nell'import/export hanno un ampio portafoglio di clienti che generano un volume significativo di dati personali.
   - Le imprese trattano dati personali particolarmente sensibili (ai sensi dell'art. 5, lett. c nLPD). Esempio: sono interessate le imprese che trattano dati personali relativi a opinioni politiche, religione, salute, dati genetici, etnia, assistenza sociale, procedimenti giudiziari, ecc.
   - Le imprese effettuano una profilazione ad alto rischio.
   - Le imprese adottano decisioni individuali automatizzate.

   In questi casi, i requisiti in termini di protezione dei dati, e in particolare di sicurezza dei dati, sono più severi rispetto alle imprese che trattano i dati di un numero limitato di dipendenti, fornitori, clienti, ecc.

   A seconda dei casi e del volume di dati personali trattati, questo lavoro di conformità richiederà lo sviluppo di una certa competenza o il ricorso ad esperti e, su base regolare, la creazione di processi interni per soddisfare i requisiti della legge. Non bisogna sottovalutare le risorse materiali

(software di gestione dei dati, ecc.), umane (nomina di un responsabile della protezione dei dati, ecc.) e il tempo necessario.

A seconda del grado di conformità, le imprese sono fortemente incoraggiate a ricorrere ai servizi di esperti informatici e avvocati, nonché alla formazione offerta dalle Camere di commercio.

4. **Sensibilizzare**
   Indipendentemente dalle dimensioni dell'impresa: tutti i dipendenti, dagli apprendisti ai responsabili di impresa, devono essere sensibilizzati sulle questioni relative alla protezione dei dati. Ricezionisti, project manager, responsabili delle risorse umane, consulenti, liberi professionisti, direttori d'impresa: i collaboratori di ogni livello di un'impresa trattano regolarmente dati personali e ne hanno la responsabilità penale.

   Né la nLPD né il GDPR richiedono esplicitamente l'organizzazione di corsi di formazione, ma nella pratica questi sono spesso necessari (e possono avere l'effetto di ridurre la responsabilità in caso di reato) per creare la necessaria consapevolezza su questo tema all'interno dell'azienda.

   Esempio: un ricezionista tiene un registro dei visitatori di un'impresa. Raccogliendo e archiviando il nome e il cognome delle persone che visitano l'azienda, il ricezionista sta già trattando dati personali.

5. **Trasparenza e informazione**
   La trasparenza nel trattamento dei dati rimane un principio importante ai sensi della nuova LPD. Esiste anche l'obbligo di fornire informazioni al momento della raccolta dei dati. Il responsabile del trattamento dei dati è tenuto a informare gli interessati su vari aspetti del trattamento dei dati. La stesura e l'aggiornamento di una dichiarazione sulla protezione dei dati è essenziale in vista dell'entrata in vigore della nLPD (sul sito web dell'impresa, ma anche nella corrispondenza).

6. **Sicurezza informatica**
   Per quanto concerne la sicurezza dei dati, le imprese devono garantire che la sicurezza dei loro sistemi informatici e delle applicazioni software soddisfi i requisiti della nuova legge. Ciò include misure tecniche e organizzative (definizione dei diritti di accesso, pseudonimizzazione dei dati, ecc.) per prevenire attacchi informatici, manipolazione e furto di dati e altre perdite di dati. Lo scopo di queste misure è quello di raggiungere gli obiettivi di protezione della sicurezza dei dati stabiliti dall'art. 2 dell'OPDa (riservatezza, disponibilità, integrità e tracciabilità).

   In questo contesto, va notato che «per tutta la durata del trattamento», vi è l'obbligo di verificare e, se necessario, adeguare le misure adottate e che una violazione intenzionale dei requisiti minimi di sicurezza dei dati è soggetta a sanzioni (art. 61, lett. c nLPD).

7. **Organizzazione e procedure interne**
   Per rispondere conformemente alle esigenze della nuova legge a qualsiasi richiesta esterna (richieste di informazioni o cancellazione dei dati personali di un cliente) o incidenti che comportano la fuga, la perdita o

l'uso improprio di dati personali, occorre stabilire procedure interne chiare nonché regolamenti o direttive. A seconda dell'incidente, questi ultimi devono definire in particolare quale/i collaboratore/i (compresi i sostituti) devono intraprendere quale/i azione/i ed entro quale/i tempo/i.

Esempio: in caso di violazione della sicurezza dei dati, le procedure dovrebbero stabilire le situazioni e i criteri per valutare se un incidente debba essere segnalato alle autorità. Tali procedure devono inoltre includere spiegazioni chiare che indichino quale collaboratore deve segnalare l'incidente, entro quale termine, in quale forma e a quale autorità. Tali procedure possono assumere la forma di liste di controllo (check-lists).

8. **Allestire un registro delle attività**
   La nLPD prevede che il titolare e il responsabile del trattamento tengano ciascuno un registro delle proprie attività. Tale obbligo vale per tutte le imprese. Il Consiglio federale può però prevedere eccezioni per le imprese con meno di 250 collaboratori (art. 12 cpv. 2 nLPD e art. 24 OPDa).

   La creazione di tali elenchi presuppone che tutti i trattamenti di dati personali all'interno di un'impresa siano identificati e raccolti sistematicamente. Soprattutto nei casi in cui tale registro non è ancora tenuto e laddove vengano eseguite molte operazioni diverse, questa procedura comporta un lavoro considerevole e dovrebbe pertanto essere avviata in una fase iniziale.

9. **Revisione dei contratti**
   Alla luce dei cambiamenti che interverranno con la nuova legge e da qui alla sua entrata in vigore, le imprese dovrebbero esaminare – e se necessario adeguare – i contratti stipulati con i propri clienti, fornitori, prestatori di servizi ma anche con i propri collaboratori. È importante agire tempestivamente. Anche una rapida attuazione ha senso, poiché è prevedibile che molti partner contrattuali a loro volta richiedano contratti – o un adattamento di contratti già esistenti – che includano clausole in linea con la nuova legge sulla protezione dei dati.

10. **Rimanere informati**
    Per comprendere le implicazioni del rispetto della nLPD, è necessario saper assimilare le problematiche e le implicazioni concrete della nuova legge sulle procedure di lavoro. Informatevi consultando i siti delle autorità garanti della protezione dei dati (IFPDT), blog e riviste specializzate e partecipate ai vari corsi di formazione (offerti, ad esempio, dalle Camere di Commercio).
    Va notato che garantire la conformità alla protezione dei dati non è un esercizio puntuale. Al contrario, quest'ultima deve essere controllata regolarmente e, se necessario, adattata, in particolare in vista degli sviluppi tecnici (ad esempio nuovi sistemi informatici), giuridici (ad esempio adeguamenti legislativi o prassi delle autorità), aziendali (ad esempio nuovi sistemi informatici) e commerciali (ad esempio nuovi servizi, nuove filiali in altri paesi). Per quanto riguarda la sicurezza dei dati, l'art. 1 cpv. 5, OPDa prescrive esplicitamente che la necessità di protezione dei dati personali, il rischio connesso nonché le misure tecniche e

organizzative debbano essere rivalutate per tutta la durata del trattamento e adattate se necessario. È importante stabilire le modalità e le responsabilità di tali verifiche.