Panoramica

Dopo un lungo tira e molla (e dopo aver aggiustato le ultime divergenze), nel corso della sua votazione finale del 25 settembre 2020 il Parlamento svizzero ha approvato la revisione totale della legge svizzera sulla protezione dei dati (LPD). Con la presente desideriamo informarvi (ancora una volta) brevemente sui retroscena del modello di legge e soprattutto sulle principali novità.

Con la revisione totale, la legge svizzera sulla protezione dei dati, ormai non più al passo con i tempi (risalente all'anno 1992), mira ad adeguarsi all'evoluzione tecnologica e sociale odierna e avvicinarsi ai regolamenti più recenti e moderni nel campo europeo della protezione dei dati (in particolare all'RGPD UE). Al centro dell'attenzione c'erano soprattutto i seguenti aspetti:

- Aumento della trasparenza e rafforzamento dei diritti delle persone interessate
- Promozione della prevenzione e della responsabilità personale dei responsabili del trattamento dei dati
- Rafforzamento del controllo sulla protezione dei dati
- Affinamento delle disposizioni penali

In seguito al messaggio e all'avamprogetto del Consiglio federale, c'erano da temere alcuni inasprimenti legali che avevano causato in molte aziende una certa incertezza giuridica e un non trascurabile supplemento di spesa per il trattamento dei dati personali. Di conseguenza, in collaborazione con l'Associazione svizzera delle società di leasing (ASSL) e i suoi partner economiesuisse e l'Unione svizzera delle arti e mestieri usam, l'UPSA si è impegnata a favore di un'attuazione liberale e funzionale della revisione, che da un lato non pregiudicasse la decisione di adeguatezza dell'UE e quindi il trasferimento dei dati tra l'UE e la Svizzera e, dall'altro, prescindesse da norme inutilmente severe che sarebbero andate al di là di quelle dell'RGPD UE (la cosiddetta "Swiss Finish"). Questo impegno ci è riuscito in ampie parti, ad es. per quanto riguarda la deroga per la gestione di un elenco dei trattamenti, così come il diritto alla comunicazione e – almeno in parte – la profilazione.

Tuttavia, in futuro si dovranno fare i conti con **norme più rigide** nel campo del trattamento dei dati personali, dei quali vi consigliamo di occuparvi tempestivamente, in modo da poter verificare e – ove necessario – adeguare la vostra procedura di protezione dei dati prima dell'entrata in vigore della revisione di legge (ad es. compilazione delle dichiarazioni sulla protezione dei dati, eventuali elenchi delle attività di trattamento, adeguamento delle procedure di trattamento dei dati, nomina di un incaricato della protezione dei dati, stipulazione di contratti per affidare il trattamento dei dati a soggetti esterni, ecc.).

Trascorso il termine di referendum di 100 giorni, il Consiglio federale deciderà sull'entrata in vigore. La legge sulla protezione dei dati revisionata (qui di seguito denominata "**revLPD**") dovrebbe quindi entrare in vigore non prima del 1º gennaio 2022, tanto più che occorre ancora adeguare la relativa ordinanza (OLPD). Vi terremo informati sulla decisione del Consiglio federale.

AGVS/UPSA
Wölflistrasse 5, 3006 Bern
Telefon 031 307 15 15, Fax 031 307 15 16
info@agvs-upsa.ch, www.agvs-upsa.ch

Principali novità

Vi preghiamo di tenere presente che nella presente comunicazione ai soci non possiamo spiegare nel dettaglio tutte le disposizioni nuove o modificate, ma ci concentreremo sulle novità che reputiamo più importanti rispetto alla legge attualmente in vigore.

- **Nessuna protezione dei dati delle persone giuridiche** Mentre la LPD in vigore è applicabile sia ai dati delle persone fisiche che a quelli delle persone giuridiche, la revLPD limita il campo d'applicazione – esattamente come l'RGPD UE – ai dati delle persone fisiche.
- **Dati personali degni di una protezione particolare** La revLPD estende l'elenco dei dati considerati particolarmente degni di protezione e quindi collegati a conseguenze giuridiche qualificate (tra le altre cose durante il consenso, la valutazione d'impatto sulla protezione dei dati, la comunicazione a terze parti così come la valutazione dell'affidabilità creditizia). Anche i dati genetici e biometrici (ad es. impronte digitali), quelli cioè che identificano in modo inequivocabile una persona fisica, sono stati qualificati come degni di una protezione particolare.
- **Profilazione e profilazione con rischio elevato** Una delle questioni più controverse e discusse dell'intero modello di legge era se includere nella legge, accanto a una profilazione "normale", anche una "profilazione con rischio elevato". Alla fine le Camere – in contrasto con le nostre raccomandazioni – hanno seguito le mozioni della conferenza di conciliazione, secondo cui la profilazione con rischio elevato doveva essere definita legalmente e sottoposta a regole speciali. Con la nuova legge, in caso di profilazione con rischio elevato, un eventuale consenso necessario deve quindi essere *esplicito*. Inoltre, decade l'interesse legittimo del responsabile e quindi la sua ragione giustificativa per una violazione della personalità, quando le sue attività di trattamento dei dati per la verifica dell'affidabilità creditizia comportano una profilazione con rischio elevato.

  Una profilazione con rischio elevato sussiste quando i dati personali vengono trattati in modo automatico e quando l'associazione dei dati consente di valutare gli "aspetti essenziali della personalità". La definizione giuridica è molto vaga e a livello pratico non sarà facile una delimitazione rispetto alla profilazione "normale". Sarà eventualmente l'ordinanza a dover fare ulteriore chiarezza in merito.

  In ogni caso, questa modifica significa che per una verifica dell'affidabilità creditizia, per la quale viene impiegata una profilazione con rischio elevato, in futuro occorrerà garantire il rispetto di tutti i principi di trattamento o l'esistenza di un'altra ragione giustificativa (in particolare il consenso da parte della persona interessata).
- **Codici di condotta** Tra le altre cose, la revLPD permette alle associazioni economiche, professionali e di categoria, che in base al loro statuto sono autorizzate a tutelare gli interessi economici dei propri soci, di presentare i codici di condotta all'Incaricato

federale della protezione dei dati e della trasparenza (IFPDT). Ciò permetterà di incentivare lo sviluppo dell'autoregolamentazione e della responsabilità personale dei responsabili. L'IFPDT dovrà quindi prendere ufficialmente posizione sui codici di condotta. Anche se da una presa di posizione positiva non è possibile far derivare nessun diritto,

si può però sempre dare per scontato che chi osservi il codice non vada incontro a provvedimenti amministrativi. In determinate circostanze, i responsabili che osservano i codici possono inoltre rinunciare allo svolgimento di una valutazione d'impatto sulla protezione dei dati. Come già sapete, l'UPSA contribuisce all'elaborazione della "carta dell'economia svizzera per una gestione responsabile dei dati" (il codice di condotta è accessibile al seguente indirizzo: https://www.economiesuisse.ch/it/gestionedati).

- **Elenchi sulle attività di trattamento dei dati** Come l'RGPD UE, la revLPD prevede, sia per il mandante che anche per il responsabile del trattamento, l'obbligo di tenere un elenco delle proprie attività di trattamento dei dati. Tale elenco deve contenere almeno i dati prescritti dalla legge. Il Consiglio federale prevede delle eccezioni per le aziende con meno di 250 collaboratrici e collaboratori e le cui attività di trattamento dei dati comportano un basso rischio di violare la personalità delle persone interessate. Queste eccezioni devono ancora essere disciplinate nell'ordinanza.
- **Responsabile del trattamento** Giusta la revLPD, il trattamento di dati personali può essere affidato a terzi mediante convenzione o per legge se – esattamente come la legge attualmente in vigore – non è diverso da quello che il mandante stesso avrebbe il diritto di fare. Come avviene nell'UE, la novità è che un conferimento delle attività di trattamento dei dati a un subfornitore è consentito solo previa autorizzazione del mandante, in modo che quest'ultimo mantenga (almeno indirettamente) il controllo sul trattamento dei dati. Il mandante deve inoltre assicurarsi che il responsabile del trattamento sia in grado di garantire la sicurezza dei dati. Per il resto non cambia molto da questo punto di vista. In particolare, la convenzione sull'affidamento del trattamento dei dati continua a non essere soggetta a nessun requisito formale particolare.
- **Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita** Come l'RGPD UE, la revLPD contiene i principi "privacy by design" e "privacy by default". Dal punto di vista tecnico e organizzativo, il mandante deve strutturare il trattamento dei dati in modo che vengano rispettate le norme sulla protezione dei dati, in particolare i principi del trattamento (privacy by design). Inoltre, deve configurare le impostazioni predefinite, ad es. nelle app o sui siti web, in modo che il trattamento dei dati personali si limiti alla misura necessaria e sufficiente per le finalità previste (privacy by default).

- **Sviluppo degli obblighi d'informazione** Giusta la revLPD, all'atto della raccolta dei dati personali occorre fornire alla persona interessata almeno le seguenti informazioni:
    - Identità e dati di contatto del responsabile
    - Finalità del trattamento
    - Eventualmente destinatarie e destinatari o categorie di destinatarie e destinatari a cui verranno comunicati i dati personali

  Se i dati personali verranno comunicati all'estero, alla persona interessata occorre comunicare anche lo Stato o l'organo internazionale ed eventualmente i garanti per la protezione dei dati personali.
- **Sviluppo degli obblighi di comunicazione** Rispetto alla LPD attualmente in vigore, la revLPD prevede obblighi di comunicazione estesi. Con la nuova legge, l'obbligo di comunicazione non si limita più alle informazioni minime definite in modo conclusivo (tra cui con la nuova legge rientreranno anche le informazioni sulla durata della conservazione, sul trasferimento all'estero e sulle decisioni individuali automatizzate), ma comprende qualsiasi informazione che è necessaria alla persona interessata per far valere i suoi diritti secondo la revLPD. Per quanto riguarda la comunicazione sui "dati personali trattati", la nuova legge prescrive che questi dati debbano essere comunicati e/o divulgati "come tali". Con ciò dovrebbe essere chiaro che il diritto alla comunicazione sancito dalla legge sulla protezione dei dati non rappresenta un diritto alla pubblicazione dei documenti e/o alla divulgazione degli atti.
- **Diritto alla portabilità dei dati** La revLPD prevede un diritto alla divulgazione e al trasferimento dei dati ("portabilità dei dati"). In base a questo diritto, la persona interessata può pretendere dal responsabile – di norma gratuitamente – la consegna dei propri dati personali in un comune formato elettronico e/o il loro trasferimento a un altro responsabile, quando il responsabile tratta i dati in modo automatico e gli stessi vengono elaborati con il consenso della persona interessata o in relazione diretta con la stipulazione o l'esecuzione di un contratto.
- **Decisione individuale automatizzata** La revLPD prevede che il responsabile sia tenuto a informare la persona interessata in merito a una decisione che avvenga esclusivamente su base automatizzata e che produca effetti giuridici o ripercussioni notevoli per la stessa. La persona interessata deve avere la possibilità di esporre il suo punto di vista e può pretendere che la decisione venga rivista da una persona fisica. Questo non vale quando la decisione è direttamente connessa alla conclusione o all'esecuzione di un contratto tra il responsabile del trattamento e la persona interessata e la richiesta di quest'ultima viene accolta o quando la persona interessata accetta espressamente che la decisione venga presa in modo automatizzato.

Quando in merito alla stipulazione di un contratto di leasing la decisione avviene in modo esclusivamente automatizzato, occorre dare la possibilità al richiedente di esporre la sua presa di posizione e di pretendere che la decisione venga rivista da una persona fisica, eccetto nel caso in cui il contratto di leasing venga accolto o il richiedente abbia espressamente accettato che la decisione venga presa in modo automatizzato.

- **Valutazione d'impatto sulla protezione dei dati** Giusta la revLPD, il responsabile è tenuto a effettuare una valutazione d'impatto sulla protezione dei dati quando il trattamento dei dati può comportare un rischio elevato per la personalità o per i diritti fondamentali della persona interessata. Un simile rischio elevato può risultare dal tipo, dall'entità, dalle circostanze e dalle finalità del trattamento. In una valutazione d'impatto sulla protezione dei dati è necessario definire il trattamento previsto e i rischi ad esso legati, così come le misure idonee per ovviarli. Sono eventualmente possibili delle eccezioni quando il responsabile osserva un codice di condotta.
- **Comunicazione in merito alla violazione della protezione dei dati** Giusta la revLPD, in caso di una violazione della protezione dei dati, i responsabili devono informare nel più breve tempo possibile l'IFPDT qualora sussista un notevole rischio per la personalità o i diritti fondamentali delle persone interessate. In questi casi, fatte salve determinate eccezioni, il responsabile è tenuto a informare anche la persona interessata, se necessario per la sua protezione o se lo pretende l'IFPDT. Il responsabile del trattamento deve comunicare nel più breve tempo possibile al mandante una violazione della sicurezza dei dati (non all'IFPDT e/o alla persona interessata).
- **Sanzioni** Giusta la revLPD, in caso di violazione intenzionale degli obblighi d'informazione e di comunicazione così come in caso di violazione intenzionale del dovere di diligenza, le persone fisiche possono essere punite con una multa fino a CHF 250'000.00 (con la legge attualmente in vigore fino a max CHF 10'000.00). In futuro, la mancata compliance della protezione dei dati non comporterà quindi solo un rischio per la reputazione dell'azienda, ma anche gravi conseguenze penali per i collaboratori giudicati responsabili.

Webinar

Cogliamo l'occasione per informarvi che il webinar sulla protezione dei dati (in tutte le lingue nazionali), che l'UPSA ha organizzato insieme all'ASSL sarà disponibile prossimamente sul sito web. Questo webinar fornisce ai partecipanti una panoramica sui principali fondamenti della legge sulla protezione dei dati così come sui (nuovi) obblighi nel trattamento dei dati. Inoltre contiene link a vari modelli di documenti.

Naturalmente, il webinar non può sostituire una consulenza legale che sarà necessaria per verificare ed eventualmente adeguare le vostre procedure di protezione dei dati.