AGVS | UPSA
Auto Gewerbe Verband Schweiz
Union professionnelle suisse de l'automobile
Unione professionale svizzera dell'automobile

SLVASSL
Schweizerischer Leasingverband
Association Suisse des Sociétés de Leasing

Conclusa la revisione delle legge federale sulla protezione dei dati (LPD)
Le nuove regole entreranno in vigore dal 1º settembre 2023

Fin dal 2017, con diverse comunicazioni informative rivolte i soci vi abbiamo tenuti al corrente in merito alla revisione totale della legge svizzera sulla protezione dei dati attualmente in corso e ai corrispondenti lavori dell'ASSL nel quadro del progetto comune con l'UPSA. Ora la revisione delle legge federale sulla protezione dei dati (LPD) si è conclusa. Il 31 agosto 2022 il Consiglio federale ha pubblicato l'ordinanza sulla protezione dei dati (OPDa) e stabilito l'**entrata in vigore delle nuove regole a partire dal 1º settembre 2023**.

L'ASSL e l'UPSA si sono impegnate a favore di una revisione della legge sulla protezione dei dati compatibile con le esigenze dell'economia e al tempo stesso con le normative UE. La nuova legge e la corrispondente ordinanza concordano in ampie parti con le regole europee. Tuttavia, nell'esame e nella messa in pratica della nuova impostazione della protezione dei dati a livello aziendale devono essere considerate alcune cosiddette peculiarità svizzere («swiss finish»).

Le imprese svizzere hanno ora un **anno di tempo per mettere in pratica le nuove regole**: non sono previsti (ulteriori) termini transitori.

Di seguito vi presentiamo brevemente una selezione delle novità che vi potrebbero riguardare più da vicino in quanto nostri soci. In allegato troverete inoltre una lista di controllo con i singoli compiti per la progressiva attuazione delle nuove norme in materia di protezione dei dati presso la vostra impresa.

1. **Nuove denominazioni dei ruoli (art. 5 lett. j e k nLPD)**

   Con le nuove norme vengono introdotti i concetti di «titolare del trattamento» e «responsabile del trattamento». Per comprendere le ulteriori considerazioni – nonché lo stesso testo di legge – è utile conoscere questi due ruoli. Per **titolare del trattamento** si intende chi […] determina lo scopo e i mezzi del trattamento, ossia per esempio un datore di lavoro nel caso del trattamento di dati personali dei propri collaboratori o un rivenditore rispetto al trattamento dei dati personali dei propri clienti. È per contro denominato **responsabile del trattamento** chi […] tratta dati personali per conto del titolare del trattamento, per esempio in caso di salvataggio dei dati su un server esterno o da parte di un fornitore di servizi cloud.

2. **Profilazione (art. 5 lett. f. nLPD)**

   Viene introdotta una distinzione tra «profilazione» e «profilazione a rischio elevato». Per **profilazione** si intende ogni trattamento automatizzato di dati personali consistente nell'utilizzazione degli stessi per valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere aspetti concernenti il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, i luoghi di permanenza e gli spostamenti di tale persona (art. 5 lett. f nLPD). La **profilazione a rischio elevato** comporta in aggiunta un rischio elevato per la personalità o i diritti fondamentali della persona interessata (art. 5 lett. g nLPD). La profilazione **non presuppone di per sé un consenso**, nemmeno in caso di

rischio elevato. Tuttavia, è rilevante in relazione agli obblighi di informare, all'obbligo di verbalizzazione e alla valutazione d'impatto sulla protezione dei dati (cfr. sotto).

3. Netta estensione degli obblighi di informazione e di fornire le informazioni richieste

Le nuove norme richiedono che le persone interessate vengano **informate** in particolare sulla raccolta di dati personali; devono essere comunicate tutte le informazioni necessarie affinché le persone interessate possano far valere i propri diritti e sia garantito un trattamento trasparente dei dati. Ciò comprende in particolare i dati di contatto del titolare del trattamento, lo scopo del trattamento e l'eventuale destinatario dei dati personali nel caso in cui questi vengano trasmessi a terzi (art. 19 nLPD). Una violazione intenzionale di tale obbligo è sanzionata penalmente.

Chiunque può domandare se dati personali che lo concernono sono oggetto di trattamento (diritto d'**accesso**). In tal caso devono essere fornite tutte le informazioni necessarie affinché la persona interessata possa far valere i suoi diritti e sia garantito un trattamento trasparente dei dati. La legge contiene un corrispondente elenco (art. 25 nLPD).

4. Decisione individuale automatizzata (art. 21 nLPD)

Una decisione individuale automatizzata è una decisione che avviene sulla base di una valutazione dei dati (p. es. condizioni come interessi, durata contrattuale, termini di pagamento o conclusione di un contratto di assicurazione o di credito ecc.) senza intervento umano e che comporta per la persona interessata effetti giuridici o conseguenze significative.

La persona interessata deve essere **informata** di tale decisione individuale automatizzata e le deve essere data la possibilità di **esprimere il proprio parere**. Salvo nel caso in cui abbia in precedenza espressamente acconsentito alla decisione automatizzata, la persona interessata può esigere che la stessa sia **riesaminata da una persona fisica**.

Nel quadro del diritto d'accesso, deve essere comunicata alla persona interessata la logica su cui si basa una decisione individuale automatizzata.

5. Obblighi amministrativi

Sono stati estesi anche gli obblighi amministrativi, che comprendono per esempio:

- la tenuta di un *registro delle attività di trattamento* (art. 12 nLPD). Un registro delle attività di trattamento è un inventario contenente i diversi trattamenti dei dati all'interno dell'impresa. Vengono registrati i diversi scopi del trattamento (p. es. gestione delle risorse umane, marketing ecc.) e le corrispondenti condizioni quadro. Le eccezioni a tale obbligo riguardano: le imprese con meno di 250 collaboratrici e collaboratori (art. 24 OPDa);

- la redazione di *valutazioni d'impatto sulla protezione dei dati* nel caso in cui il trattamento dei dati possa comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata (art. 22 nLPD);

- gli *obblighi di notifica* in caso di violazioni della legge sulla protezione dei dati (art. 24 nLPD e art. 15 OPDa);

- la *verbalizzazione* dei trattamenti automatizzati di grandi volumi di dati personali degni di particola protezione o profilazione a rischio elevato qualora le misure preventive adottate non riescano a garantire la protezione dei dati (art. 4 OPDa); nonché

- la redazione di un *regolamento per i trattamenti automatizzati*. Quest'ultimo deve inoltre essere regolarmente aggiornato se vengono trattati su grande scala dati personali degni di particolare protezione o se viene eseguita una profilazione a rischio elevato (art. 5 OPDa).

6. Sicurezza dei dati (art. 8 nLPD)

Devono essere adottati provvedimenti tecnici e organizzativi (p. es. diritti d'accesso, pseudonimizzazione) volti a garantire un'adeguata sicurezza dei dati. Ciò comporta anche che applicazioni e simili devono essere configurate in maniera che di default i dati personali siano anonimizzati e/o cancellati dopo un determinato periodo di tempo.

Se i dati personali sono trattati da un responsabile del trattamento, il titolare del trattamento deve assicurarsi che quest'ultimo sia in grado di garantire la sicurezza dei dati (p. es. tramite contratti di affidamento del trattamento dei dati a soggetti esterni).

Rispetto al tema della sicurezza dei dati vale inoltre la pena di ricordare che «per tutta la durata del trattamento» sussiste un obbligo alla verifica e all'eventuale adeguamento delle misure adottate e che una violazione intenzionale dei requisiti minimi in termini di sicurezza dei dati è sanzionabile.

7. Comunicazione di dati personali all'estero

Per comunicazione si intende in particolare anche la conservazione dei dati personali su un sistema informatico estero (server, cloud), così come l'accesso da parte di un servizio di assistenza estero.

In linea di principio, i dati personali possono essere comunicati all'estero se la legislazione dello Stato destinatario garantisce un'adeguata protezione dei dati (art. 16 cpv. 1 nLPD). L'allegato 1 dell'OPDa contiene un elenco dei Paesi in cui tali condizioni sono assicurate. In caso di comunicazione dei dati personali in *altri* Stati – in particolare anche negli Stati Uniti – si presuppone l'applicazione di una concreta eccezione o l'implementazione di misure di protezione alternative tali da garantire un'adeguata protezione dei dati (art. 16 cpv. 2 e art. 17 nLPD).

8. Sanzioni

In caso di violazione di determinati obblighi, la nuova legge sulla protezione dei dati prevede multe fino a 250 000 franchi (art. 60 segg. nLPD). Sono sanzionabili azioni e omissioni intenzionali, ma non i casi di negligenza. Diversamente dall'UE, dove le sanzioni si rivolgono contro le imprese, in Svizzera è punita in linea di principio la persona fisica responsabile. L'impresa stessa può essere sanzionata solo con una multa fino a 50 000 franchi nel caso in cui l'individuazione della persona fisica punibile all'interno dell'impresa o dell'organizzazione comporti oneri d'inchiesta sproporzionati.

Raccomandiamo di provvedere tempestivamente all'attuazione delle nuove norme affinché il 1º settembre 2023 la vostra impresa sia organizzata in maniera conforme alla nuova legge sulla protezione dei dati.

Settembre 2022