

Lista di controllo: attuazione della nuova legge sulla protezione dei dati

Quanto di seguito esposto riguarda i principali compiti necessari per l'attuazione della nuova legge federale sulla protezione dei dati (nLPD), che entrerà in vigore il 1° settembre 2023. L'attenzione si concentra sui punti che presentano una maggiore rilevanza per i soci dell'ASSL e dell'UPSAs. Non esistendo una soluzione universale valida in ogni situazione («one size fits all»), è necessario considerare separatamente ogni singolo caso. La presente lista di controllo non ha pertanto alcuna pretesa di esaustività.

- Definizione di **responsabilità e funzioni per la pianificazione del progetto** di implementazione delle nuove norme in materia di protezione dei dati.
- Redazione di un **registro dei casi di trattamento di dati personali** (cosiddetto registro delle attività di trattamento), p. es. nel campo del marketing, della gestione delle risorse umane, dell'elaborazione dei contratti ecc. Questo punto rappresenta un obbligo di legge se la vostra impresa conta più di 250 collaboratrici e collaboratori, tratta su grande scala dati personali degni di una protezione particolare o esegue una profilazione a rischio elevato (art. 12 nLPD e art. 25 OPDa). Negli altri casi il registro può essere compilato volontariamente e fungere da base per l'adempimento di ulteriori obblighi, come p. es. gli obblighi di informare le persone interessate.
- Verifica della necessità o dell'opportunità di nominare un **consulente per la protezione dei dati** (contrariamente all'RGPD, con la nLPD questa è una scelta volontaria per i privati e rappresenta un obbligo solo per gli organi federali, art. 10 nLPD).
- Redazione di **dichiarazioni concernenti la protezione dei dati** – per il sito web, per le attività dell'impresa e per il personale (così come per chi invia la propria candidatura) – mirate all'adempimento degli obblighi di informare le persone interessate (art. 19 nLPD e art.13 OPDa).
- Verifica e aggiornamento delle misure per la **sicurezza dei dati** (art. 8 nLPD e art. 1 segg. OPDa), in particolare i provvedimenti tecnici e organizzativi per la sicurezza dei dati (art. 3 OPDa), la verbalizzazione (art. 4 OPDa) e la tenuta di un registro delle attività di trattamento automatizzate (art. 5 segg. OPDa).
- Elaborazione di **regolamenti e processi per il rispetto dei diritti delle persone interessate**, in particolare per la notifica di violazioni della sicurezza dei dati (art. 24 nLPD e art. 15 OPDa), la conservazione e la cancellazione dei dati (art. 6 cpv. 4 nLPD), il diritto d'accesso (art. 25 nLPD e art. 16 segg. OPDa), così come il diritto alla portabilità dei dati (art. 28 nLPD e art. 20 segg. OPDa).
- Verifica e aggiornamento di **contratti di affidamento del trattamento dei dati a terzi** (art. 9 nLPD e art. 7 OPDa), in particolare nell'ottica della trasmissione transfrontaliera (art. 16 nLPD e art. 8 segg. OPDa). Eventuale verifica e aggiornamento degli accordi interni al gruppo in materia di trasmissione dei dati.

- Verifica e aggiornamento di altri accordi (con clienti, fornitori, collaboratori ecc.) in materia di protezione dei dati.
- 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 lett. f nLPD e art. 14 OPDa).
- Definizione e svolgimento di **corsi di formazione** per il personale. Questa misura non è richiesta esplicitamente né dall'RGPD né dalla LPD, ma è spesso necessaria per generare la necessaria sensibilità rispetto all'argomento all'interno dell'impresa. I corsi di formazione possono essere svolti dall'impresa stessa oppure da soggetti esterni, come p. es. l'ASSL in collaborazione con la Business Academy UPSA. Potete trovare le nostre offerte alla pagina: [Webinar LPD](#).
- Definizione di **procedure e responsabilità per il regolare controllo e aggiornamento** della conformità in materia di protezione dei dati.

Settembre 2022