Kellerhals Carrard

Conclusione della revisione totale della Legge federale sulla protezione dei dati (LPD).
Le nuove regole si applicano a partire dal 1° settembre 2023

Check-list: Attuazione della nuova legge sulla protezione dei dati

I commenti che seguono si riferiscono ai compiti più importanti necessari per l'attuazione della nuova legge federale sulla protezione dei dati (nLPD), che entrerà in vigore il 1° settembre 2023. Non esiste una soluzione unica per tutti, ogni singolo caso deve essere considerato separatamente. La lista di controllo non ha quindi la pretesa di essere esaustiva.

- Determinare responsabilità e funzioni per la pianificazione del progetto di implementazione delle nuove norme sulla protezione dei dati.
- Creare un registro dei trattamenti dei dati personali (il cosiddetto registro dei trattamenti), ad esempio nelle aree del marketing, delle risorse umane, nella stesura di contratti, ecc. Si tratta di un obbligo legale se la vostra azienda ha più di 250 dipendenti, tratta dati personali degni di particolare protezione su larga scala o effettua una profilazione a rischio elevato (art. 12 nLPD e art. 24 OLPD). In altri casi, il registro può essere tenuto volontariamente e servire come base per l'adempimento di altri obblighi, come il dovere di informare gli interessati.
- Verificare se è necessario o opportuno nominare un consulente per la protezione dei dati (a differenza del RGPD, in applicazione della nLPD per i privati questo è facoltativo - solo gli organi federali sono obbligati per legge a farlo, art. 10 nLPD).
- Redigere dichiarazioni sulla protezione dei dati per il sito web, per le attività dell'azienda e per i dipendenti (nonché per candidati) al fine di adempiere agli obblighi di informazione nei confronti degli interessati (art. 19 nLPD e art. 13 OLPD).
- Rivedere e aggiornare le misure di sicurezza dei dati (art. 8 nLPD e art. 1 e segg. OLPD), in particolare le misure di sicurezza tecniche e organizzative dei dati (art. 3 OLPD), la registrazione (art. 4 OLPD) e l'elaborazione di un regolamento per il trattamento automatizzato dei dati (art. 5 e segg. OLPD).
- Elaborare regolamenti e processi per garantire il rispetto dei diritti degli interessati, in particolare la segnalazione di violazioni della protezione dei dati (art. 24 nLPD e art. 15 OLPD), la conservazione e la cancellazione dei dati (art. 6 n. 4 nLPD), il diritto d'accesso (art. 25 nLPD e art. 16 e segg. OLPD) e il diritto alla portabilità dei dati (art. 28 nLPD e art. 20 e segg. OLPD).
- Rivedere e aggiornare i contratti di trattamento dei dati con terzi (art. 9 nLPD e art. 7 OLPD), in particolare per quanto riguarda le comunicazioni transfrontaliere (art. 16 nLPD e art. 8 e segg. OLPD). Se necessario, rivedere e aggiornare gli accordi di trasferimento dei dati all'interno del gruppo.
- Rivedere e aggiornare altri accordi (con clienti, fornitori, dipendenti, ecc.) per quanto riguarda gli aspetti della protezione dei dati.
- Redigere valutazioni d'impatto sulla protezione dei dati se un trattamento può comportare un rischio elevato per la personalità o i diritti fondamentali dell'interessato (art. 22 f. nLPD e art. 14 OLPD).
- Determinare e attuare una formazione per i dipendenti. Sebbene ciò non sia esplicitamente richiesto dal RGPD o dalla nLPD, è spesso necessario per creare la necessaria sensibilità per l'argomento all'interno dell'azienda.
- Stabilire procedure e responsabilità per la verifica e l'aggiornamento periodici della compliance in ambito di protezione dei dati.