Promemoria sulla nuova Legge sulla protezione dei dati

Aggiornato al: 01.09.2023

La nuova Legge sulla protezione dei dati è entrata in vigore venerdì 1° settembre 2023 e ci si deve attenere da subito. Verificate con l'aiuto della nostra lista di controllo a pagina 4 a che punto è la vostra azienda in materia di protezione dei dati[1].

Definizioni importanti illustrate in sintesi:

Cosa sono i dati personali?

Tutte le informazioni che si riferiscono a una persona fisica determinata o determinabile.
Ad es.: nome, indirizzo, indirizzo di posta elettronica, numero di telefono, indirizzo IP

Cosa significa trattamento?

Qualsiasi operazione compiuta sui dati personali. Esempi: acquisizione, salvataggio, conservazione, utilizzo, modifica, comunicazione, archiviazione, cancellazione o distruzione

Io imprenditore o imprenditrice cosa devo fare?

1) **Farsi un'idea (registro del trattamento dei dati)**

   Fatevi un'idea generale delle attività di trattamento dei dati che si svolgono nella vostra azienda, senza dimenticare che qualsiasi operazione sui dati che si riferiscono a persone determinate o determinabili costituisce una forma di trattamento dei dati.
   Annotate in un registro scritto (registro del trattamento dei dati) le categorie di dati che trattate e le finalità per cui lo fate, dove archiviate i dati e quando li cancellate. Conservate il registro con cura e aggiornatelo regolarmente. Il registro vi fornisce una panoramica e non dev'essere pubblicato.

[1]Il presente contributo svolge funzione di primo orientamento e di autovalutazione. I consigli che dispensiamo non hanno alcuna pretesa di esaustività e non forniamo garanzie al riguardo. Per stabilire se la vostra azienda soddisfa effettivamente tutti i requisiti di legge è necessaria una valutazione caso per caso.

2) Informare (informativa sulla privacy)

Con un'informativa sulla privacy comunicate alle persone interessate quali categorie di dati trattate e per quali finalità e a quali categorie di destinatari trasmettete dati personali. Informate le persone interessate se trasmettete i loro dati all'estero – si pensi ad es. a soluzioni in cloud o servizi IT con server all'estero. Mettete a disposizione delle persone interessate i vostri dati di contatto, affinché possano contattarvi per qualsiasi domanda o richiesta in materia di protezione dei dati.

3) Garantire la sicurezza dei dati

Individuate, in base al vostro registro del trattamento dei dati, gli ambiti in cui sussistono rischi per le persone interessate (ad es. clienti e collaboratori o collaboratrici) e gli idonei accorgimenti tecnici e organizzativi per voi accettabili che vi permettano di minimizzare tali rischi. Ad es.: protezione con password e antivirus, piano delle autorizzazioni, cifratura dei dati, direttive interne per la protezione dei dati, adeguamento di contratti ecc.. Nel caso in cui un'operazione di trattamento dei dati possa costituire un rischio elevato per le persone interessate, è necessario procedere a una valutazione d'impatto sulla protezione dei dati (analisi dei rischi).

4) Predisporre piano delle autorizzazioni e di cancellazione

Predisponete un idoneo piano delle autorizzazione e di cancellazione. Tenete però conto degli obblighi di conservazione previsti dalla legge e dei vostri interessi legittimi alla conservazione (es. per difendersi da eventuali pretese).

5) Adeguare e predisporre contratti

Verificate nell'ambito di quali procedure trasmettete dati a terzi (es. outsourcing) e obbligate i destinatari al rispetto della protezione dei dati con un contratto per responsabili del trattamento.

6) Rispetto dei principi di base

In qualsiasi operazione concernente i dati personali (trattamento) è necessario osservare i principi di base della LPD (artt. 6 e 8 LPD). È necessario osservare tutti i principi di base. Per i collaboratori e le collaboratrici, al centro si trovano però funzionalità e proporzionalità. Secondo il principio di proporzionalità, l'acquisizione e il trattamento di dati personali può avere luogo solo per una finalità determinata. Dovete informare le persone interessate in merito alla finalità e, in linea di principio, cancellare i dati una volta che è stata raggiunta. Il principio di proporzionalità si può spiegare semplicemente con il principio di minimizzazione dei dati. Trattate dati quanto meno possibile. Tale regola si riferisce alla quantità di dati (meno in termini di volume), al periodo di conservazione (meno in termini di tempo) o alla quantità di persone che si occupano del trattamento (meno in termini di autorizzati all'accesso = «need to know»). Conseguentemente dev'essere attuato, come detto al punto 5, un piano delle autorizzazioni e di cancellazione. Particolarmente degno di nota è anche il principio della sicurezza dei dati, il quale richiede che sia garantita una sicurezza dei dati adeguata al rischio.

7) Garantire la sicurezza dei dati all'estero

Verificate se trasferite dati all'estero e se in tale Paese è garantita un'adeguata protezione dei dati (di regola tale sicurezza è data per i Paesi UE). Qualora vengano trasmessi dati in altri Paesi, sono necessarie misure di portata maggiore come ad es. l'impiego di clausole contrattuali standard.

8) Rispettare la procedura di notificazione

Qualora dovesse accadere che la sicurezza dei dati venga violata (es. e-mail inviata a gruppo di destinatari sbagliato, cybercrime, perdita di dati ecc.), verificate quanto prima se sia necessaria e opportuna una segnalazione all'IFPDT o alle persone interessate.

9) Rispetto dei principi generali di trattamento

- Trattate solo i dati necessari e cancellateli non appena non vi servono più.
- Trattate i dati solo per la finalità preventivamente comunicata.
- Comunicate in modo trasparente i dati che trattate e la finalità del trattamento nonché i soggetti e i Paesi cui li inoltrate.
- Custodite i dati al sicuro.

Lista di controllo sulla nuova protezione dei dati

Aggiornato al: 01.09.2023

Fase 1: progettazione

- rilevamento e registro del trattamento
- sicurezza dei dati (accorgimenti tecnici e organizzativi)

Fase 2: accorgimenti con effetto all'esterno

- stesura di un'informativa sulla privacy (obbligo d'informazione)
- salvaguardia dei diritti delle persone interessate
- predisposizione di un piano per la cancellazione
- regolamentazione del trasferimento di dati all'estero

Fase 3: accorgimenti con effetto all'interno

- stesura di un contratto per responsabili del trattamento
- introduzione di regolamenti e corsi per collaboratori e le collaboratrici
- effettuazione di una valutazione d'impatto sulla protezione dei dati
- predisposizione di un processo relativo all'obbligo di notificazione
- predisposizione di un processo relativo a portabilità dei dati / limite di archiviazione