Associazione Professionale Svizzera
APS TSO
Tecnici di sala operatoria diplomati SSS
Dipl. Fachfrauen/-männer Operationstechnik HF
Techniciens en salle d'opération diplomés ES

Scheda informativa sulla protezione dei dati
Attuazione della nuova legge sulla protezione dei dati a partire dal 1 settembre 2023

Per le organizzazioni, i dipendenti o i lavoratori autonomi che trattano prevalentemente dati personali che richiedono una protezione particolare (ad es. dati sulla salute)

1. Protezione dei dati / Sintesi introduttiva

L'attuale legge federale sulla protezione dei dati (LPD; in vigore dal 1992) e la relativa ordinanza mirano a proteggere la personalità e i diritti fondamentali delle persone fisiche i cui dati personali sono trattati.

Questa scheda informativa illustra il significato di protezione dei dati e cosa significa in particolare per i responsabili che lavorano o trattano dati personali particolarmente sensibili (in particolare dati sulla salute).

La nuova legge sulla protezione dei dati, che entrerà in vigore il 1 settembre 2023, prevede una protezione ancora migliore dei dati personali. Le innovazioni più importanti, come l'ampliamento dei "dati particolarmente sensibili", la "profilazione ad alto rischio", la "protezione dei dati attraverso la tecnologia", la dichiarazione di protezione dei dati sul sito web, l'elenco delle attività di trattamento in determinati casi o le multe, sono discusse di seguito.

Chi ha già trattato correttamente i dati personali in conformità con l'attuale legge sulla protezione dei dati non dovrà affrontare grossi problemi con la nuova legge sulla protezione dei dati. Tuttavia, è necessario tenere in considerazione i seguenti punti.

2. Scopo e finalità della protezione dei dati

La protezione dei dati si occupa dell'autodeterminazione informativa e della protezione contro il trattamento improprio dei dati che limita le persone fisiche nella loro personalità o nei loro diritti fondamentali. Lo scopo della legge sulla protezione dei dati è sempre stato quello di proteggere questi diritti definendo le linee guida per il trattamento e l'elaborazione dei dati personali.

3. Nuova legge sulla protezione dei dati (LPD) a partire dal 1 settembre 2023

Il 1° settembre 2023 entreranno in vigore la legge sulla protezione dei dati (LPD) completamente rivista, le disposizioni di attuazione nella nuova ordinanza sulla protezione dei dati (OPDa) e la nuova ordinanza sulle certificazioni di protezione dei dati (OCPD).

La revisione della legge sulla protezione dei dati e le corrispondenti disposizioni delle ordinanze garantiranno in futuro una protezione (ancora) migliore dei dati personali. In particolare, la protezione dei dati viene adattata agli sviluppi tecnologici, l'autodeterminazione sui dati personali viene rafforzata e la trasparenza nell'acquisizione dei dati personali viene aumentata.

La nuova legge sulla protezione dei dati garantisce la compatibilità con la legislazione europea (GDPR) in particolare. Gli adeguamenti della nuova legge sulla protezione dei dati sono importanti per garantire che l'UE continui a riconoscere la Svizzera come Paese terzo con un livello adeguato di protezione dei dati e che i trasferimenti transfrontalieri di dati siano possibili anche in futuro senza ulteriori requisiti.

3.1 Cosa rimane invariato?

Le modalità di trattamento dei dati ai sensi della nuova legge sulla protezione dei dati non cambiano in modo sostanziale. Come in precedenza, non è richiesto alcun consenso esplicito o altra giustificazione per il trattamento dei dati personali generali, a condizione che:

- siano rispettati i principi di trasparenza del trattamento - in particolare l'adempimento degli obblighi di informazione -, limitazione delle finalità, proporzionalità e sicurezza dei dati,
- l'interessato non si è opposto al trattamento (in anticipo)
- e non vengono comunicati a terzi dati personali particolarmente sensibili.

Come in precedenza, il consenso esplicito è richiesto all'interessato al momento della raccolta dei dati solo se vengono trattati dati personali particolarmente sensibili (ad esempio, dati sulla salute).

Garantire che tutti i dati personali siano cancellati o resi anonimi non appena non sono più necessari per le finalità che ne hanno giustificato il trattamento.

3.2 I cambiamenti e le innovazioni più importanti

- **Ambito di applicazione personale e materiale (art. 2 LPD)**

La nuova legge sulla protezione dei dati (LPD) e la relativa ordinanza si applicano come prima al trattamento dei dati personali da parte di privati e organi federali. Di conseguenza, sono interessate le aziende private, ma anche le associazioni e, in linea di principio, i privati che elaborano dati di persone fisiche.

In futuro, la nuova LPD non sarà più applicabile ai dati delle persone giuridiche. Pertanto, solo i dati delle persone fisiche saranno interessati e protetti.

- **Ampliamento dei dati personali "particolarmente sensibili" (art. 5 LPD)**

I dati su opinioni o attività religiose, ideologiche, politiche o sindacali; i dati sulla salute, sulla privacy e sull'appartenenza a un gruppo etnico o razziale; i dati su procedimenti o sanzioni amministrative e penali e i dati sulle misure di assistenza sociale continuano a essere considerati dati personali "particolarmente sensibili".

Il catalogo esistente dei dati personali "particolarmente sensibili" sarà ampliato. Sono ora inclusi anche i dati di identificazione registrabili digitalmente, come i dati biometrici, le impronte digitali, scansione della retina e dati genetici registrati.

- **Profilazione / profilazione a rischio elevato (art. 5 LPD)**

Si parla ora di "profilazione", ovvero di qualsiasi trattamento automatizzato dei dati.

Profilazione è il termine usato per descrivere i dati personali che possono essere utilizzati per costruire un'immagine accurata di una persona. Si tratta di caratteristiche come il luogo di residenza, gli hobby e gli interessi di una persona. Ma anche dati come l'andamento delle prestazioni lavorative, la situazione economica o le informazioni sullo stato di salute di una persona.

Si parla di "profilazione a rischio elevato" quando la profilazione comporta un rischio elevato per la personalità o i diritti fondamentali dell'interessato, in quanto porta a un collegamento di dati che consente di valutare aspetti essenziali (ad esempio, i tratti) di una persona fisica. In futuro, tali dati potranno ancora essere trattati con un alto grado di sensibilità, ma solo se non violano esplicitamente i diritti personali e se l'interessato ha dato il proprio consenso esplicito.

- **Protezione dei dati personali fin dalla progettazione e per impostazione predefinita (art. 7 LPD)**

Il principio della protezione dei dati fin dalla progettazione ("privacy by design") significa che i sistemi utilizzati per il trattamento dei dati personali devono essere progettati fin dall'inizio in modo da rispettare la protezione dei dati.

Il principio della protezione per impostazione predefinita ("privacy by default") significa che i responsabili del trattamento dei dati devono selezionare le impostazioni predefinite del software o del dispositivo in modo tale che il trattamento dei dati personali sia limitato al minimo necessario per lo scopo previsto (possono essere impostati solo i cookie assolutamente necessari per il servizio). Tutti i software, gli hardware e i servizi devono essere configurati in modo da proteggere i dati e tutelare la privacy degli utenti.

- **Cookies**

La nuova legge sulla protezione dei dati in Svizzera non rende obbligatori i cookie banner, ma impone l'obbligo di informare sull'uso dei cookie (i cookie banner o cookie layer sono strumenti utilizzati sui siti web e nelle app per ottenere il consenso degli utenti al trattamento dei dati. Con un banner di questo tipo, gli utenti dovrebbero essere in grado di accettare o rifiutare specificamente i cookie). La Svizzera non adotta quindi la direttiva UE sui cookie. Pertanto, è fondamentalmente conforme alla legge non impostare un cookie banner sui siti web svizzeri.

Tuttavia, i gestori di siti web svizzeri sono obbligati a informare sull'uso dei cookie, ma in genere possono crearli senza un consenso esplicito.

Tuttavia, se sul sito web viene generato traffico dall'UE, ossia vengono offerti prodotti/servizi anche a persone provenienti dall'UE, è obbligatorio impostare un banner per conformarsi al GDPR (vedere punto 3). In caso di dubbio, si raccomanda di impostare un banner corrispondente (ad esempio, in caso di pendolari transfrontalieri o di congressi internazionali).

- **Obbligo di fornire informazioni quando si ottengono dati personali, dichiarazione sulla protezione dei dati (art. 19 LPD)**

L'obbligo di informazione è stato ampliato rispetto alla legge precedente. I responsabili del trattamento dei dati devono ora informare adeguatamente gli interessati su ogni raccolta di dati, e non solo sui dati che richiedono una protezione speciale, come avveniva in precedenza.

La nuova legge sulla protezione dei dati non contiene un elenco esaustivo di tutte le informazioni obbligatorie che devono essere fornite all'interessato durante la procedura di appalto. Come minimo, devono essere fornite le seguenti informazioni obbligatorie:

- L'identità e i dati di contatto del responsabile della società/associazione o del lavoratore autonomo che tratta i dati.
- Le finalità del trattamento
- In caso di diffusione dei dati: i destinatari o le categorie di destinatari
- in caso di divulgazione dei dati all'estero, inoltre: lo Stato o l'organismo internazionale e, se del caso, la garanzia di un'adeguata protezione dei dati o l'eccezione in caso di assenza di tali garanzie
- in caso di raccolta indiretta di dati (cioè di dati non raccolti presso l'interessato stesso, inoltre: le categorie di dati personali trattati)
- l'esecuzione di decisioni individuali automatizzate, ossia una decisione che si basa esclusivamente su un trattamento automatizzato e che comporta una conseguenza giuridica per l'interessato o lo riguarda in modo significativo.

La LPD non specifica il modo in cui le informazioni devono essere fornite all'interessato. Non esiste un obbligo di forma legale, ma è necessario scegliere una forma appropriata che soddisfi lo scopo di un trattamento trasparente dei dati. A tal fine, si raccomanda di inserire una dichiarazione sulla protezione dei dati nel sito web.

Il modulo di contatto sul sito web deve contenere un'indicazione obbligatoria dello scopo per il quale saranno utilizzati i dati personali forniti.

- **Elenco delle attività di trattamento (solo) in determinati casi (Art. 12 LPD)**

Le organizzazioni con 250 o più dipendenti devono tenere un inventario di tutte le lavorazioni.

Le organizzazioni con meno di 250 dipendenti (cioè le piccole organizzazioni/lavoratori autonomi) devono tenerne uno solo se trattano dati personali sensibili (ad esempio, dati sulla salute).

In questo caso, il responsabile del trattamento deve tenere un registro di tutte le attività di trattamento. Se il trattamento dei dati è delegato a un incaricato, il responsabile del trattamento e l'incaricato devono tenere un registro separato:

- L'elenco della persona responsabile deve contenere informazioni sulla

- Identità della persona responsabile
- la finalità del trattamento
- una descrizione delle categorie di interessati
- le categorie di dati personali trattati
- le categorie di destinatari
- se possibile, il periodo di conservazione dei dati personali o i criteri per determinarlo
- se possibile, una descrizione generale delle TOM (Misure Tecniche e Organizzative)
- e, se i dati vengono divulgati all'estero, l'indicazione dello Stato e le garanzie di cui all'art. 16 cpv. 2 LPD.

- L'elenco del processore dell'ordine, invece, contiene "solo" informazioni:

- sull'identità del processore e del controllore
- alle categorie di trattamento effettuate per conto del responsabile,
- nonché i dettagli dei TOM e, nel caso di scambio di dati all'estero, i dettagli dello Stato

I dati personali trattati negli studi medici o dentistici, ad esempio, comprendono: Dati anagrafici e dati di contatto di pazienti, dipendenti, referenti di fornitori di servizi o di altre strutture sanitarie (ad esempio, nome, numero di telefono, indirizzo, indirizzo e-mail o data di nascita); registrazioni sul corso del trattamento, descrizioni dei sintomi, diagnosi, prescrizioni, reazioni, risultati di laboratorio, Radiografie, farmaci, dati sulla privacy come lo stato di salute, la vita sessuale o lo stato emotivo, dati sui dipendenti e sul rapporto di lavoro, comprese le valutazioni delle prestazioni e le buste paga (queste ultime sono rilevanti anche per i responsabili interni delle risorse umane).

- **Ampliamento dei diritti dell'interessato: diritto alla divulgazione dei dati (art. 25 LPD)**

Oltre all'obbligo di fornire informazioni, la LPD amplia ulteriormente i diritti degli interessati. Analogamente al GDPR, l'interessato ha ora diritto alla divulgazione e al trasferimento dei dati. Gli interessati possono richiedere che i dati da loro divulgati vengano rilasciati in un formato elettronico comune (entro 30 giorni).

In ogni caso, vengono comunicate le seguenti informazioni:

- l'identità e i dati di contatto della persona responsabile
- i dati personali trattati in quanto tali
- gli scopi della lavorazione
- il periodo di conservazione
- le informazioni disponibili sull'origine dei dati personali

Se il titolare del trattamento ha dati personali trattati da un incaricato del trattamento, il titolare del trattamento rimane obbligato a fornire informazioni.

Si raccomanda di preparare una procedura per rispondere rapidamente alle eventuali richieste di informazioni da parte delle persone interessate.

- **Notifica delle violazioni all'IFPDT (art. 24 LPD)**

In base alla nuova LPD, i responsabili del trattamento dei dati devono segnalare al più presto all'IFPDT (Incaricato federale della protezione dei dati e delle informazioni) e a tutte le parti potenzialmente interessate una violazione dei dati (ad es. perdita di dati, attacco informatico) che possa comportare un rischio elevato per la personalità o i diritti fondamentali dell'interessato, al fine di evitare sanzioni o altre complicazioni.

- **Consulente per la protezione dei dati (art. 10 LPD)**

Le aziende private possono facoltativamente nominare un consulente per la protezione dei dati ai sensi dell'art. 10 della LPD. Questi possono, ma non necessariamente, avere un rapporto di lavoro con l'azienda.

I consulenti per la protezione dei dati devono poter portare il loro punto di vista all'attenzione della direzione aziendale in caso di divergenze di opinione. Le responsabilità per la protezione dei dati e la sicurezza delle informazioni possono e devono essere regolamentate in ogni azienda indipendentemente dalla nomina di un consulente per la protezione dei dati ai sensi dell'art. 10 della LPD.

Se viene nominato un consulente per la protezione dei dati, il suo nome e i suoi dati di contatto devono essere inclusi nella dichiarazione sulla privacy.

- **Responsabilità penale / multe**

Per quanto riguarda la responsabilità penale, si deve tenere conto in particolare del fatto che dal 1 settembre 2023 la violazione di alcuni doveri darà luogo a responsabilità penale, che non riguarderà la società, ma la persona fisica responsabile. I responsabili possono essere i membri della direzione e altre persone che prendono decisioni all'interno dell'azienda o anche le persone che hanno commesso una violazione dei doveri (ad esempio, una violazione della riservatezza). Secondo la legge svizzera, tuttavia, solo la commissione intenzionale è punibile.

In caso di violazione degli obblighi di informazione, divulgazione e collaborazione (art. 60 LPD) o di violazione degli obblighi di diligenza (art. 61 LPD), le persone possono essere multate fino a 250.000 franchi svizzeri. È coperta solo la commissione intenzionale, non anche la negligenza. Per dolo si intende l'esecuzione dell'atto con consapevolezza e volontà. Una persona che ritiene possibile la realizzazione del reato e la accetta (il cosiddetto dolo eventuale) agisce già intenzionalmente.

- **Responsabilità (da distinguere dalla multa penale)**

Come già nel LPD esistente, ma a differenza del GDPR, non è l'azienda a essere responsabile della violazione del LPD, ma la persona fisica all'interno dell'azienda responsabile della violazione.

Tuttavia, il dispaccio sulla nuova LPD chiarisce che l'attenzione non è rivolta alla persona responsabile dell'azione, ma alla persona responsabile dell'organizzazione. La responsabilità dei dirigenti è chiarita con il riferimento all'art. 6 del Codice penale nell'art. 64 della LPD. Questo è l'unico modo per garantire che le persone in posizione dirigenziale siano responsabili delle violazioni e non il dipendente appena assunto.

4. Raccomandazioni

- Controllare le impostazioni (esistenti) di "protezione dei dati mediante tecnologia" e "impostazione predefinita favorevole alla protezione dei dati", compresi i cookie, come indicato alle pagine 3/4.
- Rivedere e adattare le dichiarazioni sulla privacy presenti sul sito web, come indicato a pagina 4.
- Revisione delle responsabilità organizzative per la protezione dei dati
- Redigere un repertorio di lavorazione, se necessario (pagina 5)
- Revisione della documentazione delle misure per garantire la sicurezza dei dati
- Verifica che tutte le elaborazioni dei contratti da parte di terzi siano garantite contrattualmente.
- Definizione dei processi per la gestione delle richieste di informazioni, rettifica e cancellazione e delle obiezioni al trattamento dei dati
- Definizione dei processi di notifica delle violazioni dei dati (pagina 7)
- Definizione dei processi di cancellazione e archiviazione dei dati
- Informare i dipendenti interessati del loro dovere di riservatezza professionale.