

Promemoria per terapisti/i relativo alla REVISIONE DELLA NORMATIVA SULLA PROTEZIONE DEI DATI

Premessa

La legge sulla protezione dei dati completamente rivista (nLPD) entra in vigore il 1° settembre 2023. L'obiettivo della revisione era quello di adeguare la legge sulla protezione dei dati alla normativa europea e di rafforzare i diritti delle persone interessate in termini di autodeterminazione e trasparenza. Il presente promemoria illustra le novità più importanti e la necessità di intervento.

Panoramica delle principali modifiche a partire dal 1° settembre 2023

1. Chi elabora dati, deve tenere un **registro delle attività di trattamento**.
2. Per ogni raccolta di dati deve esserci una **persona responsabile alla legge sulla protezione dei dati**.
3. La protezione dei dati va garantita da **provvedimenti tecnici**.
4. Chi tratta dati, deve **informare le persone interessate** e fornire informazioni su richiesta.
5. I dati devono essere conservati in modo da poter essere riprodotti in modo utilizzabile e anche inviati (**«portabilità dei dati»**).
6. La **cancellazione dei dati** è ora esplicitamente regolamentata: chiunque tratti dati deve anche eliminarli tempestivamente.
7. Sanzione prevista in caso di infrazioni intenzionali: **Multa** fino a CHF 250'000.00 possibile.

Spiegazioni

La revisione della legge sulla protezione dei dati impone nuovi obblighi, descritti nel presente promemoria. Le domande più frequenti (FAQ) trovano risposta in un documento separato. Le basi giuridiche figurano nella Legge federale sulla protezione dei dati (LPD) e nell'Ordinanza sulla protezione dei dati (OPDa) e di conseguenza sono collegate tra loro tramite link.

1. Obbligo di tenere un registro delle attività di trattamento ([Art. 12 nLPD](#))

La legge richiede ora la tenuta e il continuo aggiornamento di un **registro** di ogni attività di trattamento. Conformemente all'[art. 24 nLPD](#) le imprese con meno di 250 dipendenti sono esonerate da questo obbligo, a meno che venga trattata *una grande quantità di dati personali degni di particolare protezione*. Poiché i dati concernenti la salute sono considerati degni di particolare protezione, si raccomanda vivamente ai terapisti, di tenere un tale registro, indipendentemente da un obbligo legale.

2. Persona responsabile in base alla legge sulla protezione dei dati

In base alla legge sulla protezione dei dati, lo studio (l'impresa) è considerato il responsabile del trattamento dei dati e i terapisti sono responsabili dell'attuazione della protezione dei dati all'interno dell'impresa. Il trattamento dei dati personali può essere trasferito a un incaricato del trattamento (p.es. servizi cloud per la memorizzazione di dati, contabilità finanziaria esternalizzata, fornitori di software tariffa 590). Se viene incaricato un incaricato del trattamento, il responsabile del trattamento in base alla legge sulla protezione dei dati (lo studio) rimane responsabile dei dati e deve controllare e garantire che l'incaricato del trattamento elabori i dati solo in conformità alle sue specifiche e istruzioni. Il trattamento contrattuale deve essere regolato contrattualmente e includere le corrispondenti dichiarazioni sulla protezione dei dati ([art. 9 nLPD](#)).

3. Provvedimenti tecnici e organizzativi per la sicurezza dei dati ([art. 8 nLPD](#))

Per provvedimenti tecnici si intendono i diritti d'accesso interni (chi può accedere a quali dati) e la protezione contro accessi esterni (p.es. firewall, password). Grazie a questi provvedimenti, possono accedere a dati personali soltanto le persone che necessitano dell'accesso per svolgere il loro lavoro.

Qualora *dati personali vadano persi, vengano eliminati, modificati o resi accessibili (per esempio tramite furto) a terze persone (persone non autorizzate)* e in seguito a questa violazione la persona interessata corra un alto rischio di subire conseguenze negative, ciò va notificato all'Incaricato federale della protezione dei dati e della trasparenza IFPDT.

Invio di dati particolarmente riservati: al momento dell'invio, è necessario adottare provvedimenti in grado di impedire a terzi non autorizzati di accedervi, segnatamente l'invio criptato.

4. Diritto di accesso / obbligo di informazione ([art. 25 nLPD](#))

Laddove vengono raccolti dati, deve esistere un'**informativa sulla privacy**. L'informativa sulla privacy deve contenere almeno i dati di contatto della persona responsabile, lo scopo del trattamento ed eventualmente il destinatario dei dati. Un'avvertenza sul sito web o nella documentazione scritta deve informare sul luogo in cui è possibile consultare/ritirare l'informativa sulla privacy. È irrilevante se la persona interessata consulto o meno l'informativa.

I dati personali devono essere consegnati alle persone interessate entro 30 giorni dalla richiesta. Occorre garantire che i dati possano essere trovati entro un periodo di tempo ragionevole ed essere consegnati alla persona interessata in forma elettronica (cfr. 5. portabilità dei dati).

5. Portabilità dei dati ([art. 28 nLPD](#))

Le persone interessate hanno ora il diritto di richiedere i propri dati personali in un formato elettronico usuale o di farli trasferire a terzi. La consegna o la trasmissione deve di regola essere effettuata gratuitamente, se ciò non richiede un onere sproporzionato. Per «formato elettronico» usuale s'intende un formato che permetta la lettura automatica dei dati in un sistema informatico in forma strutturata (p.es. come file PDF, EXCEL, XML ecc.). Se i documenti non sono archiviati elettronicamente e sono disponibili solo fisicamente, essi devono essere scansionati e consegnati nel formato PDF.

6. Cancellazione di dati ([art. 6 cpv. 4 nLPD](#))

Per motivi di proporzionalità, i dati personali possono essere trattati finché sono **necessari** per lo scopo perseguito. In seguito, essi vanno distrutti o resi anonimi. Una conservazione troppo lunga dei dati costituisce una violazione della protezione dei dati.

Sono applicabili le scadenze di conservazione legali. **Le cartelle dei pazienti** vanno di regola conservate 20 anni. I dati più vecchi dei pazienti non più in cura vanno cancellati.

I documenti in materia di diritto del lavoro devono essere cancellati al più tardi entro 10 anni dall'uscita dall'azienda; i documenti non più necessari, come la documentazione di candidatura, vanno eliminati immediatamente dopo la cessazione del rapporto di lavoro.

Se esistono obblighi legali di conservazione dei dati, non è possibile soddisfare la richiesta di cancellazione.

7. Violazioni / sanzioni

In caso di azione od omissione deliberata (intenzionale) può essere comminata ai privati una multa fino a CHF 250'000.--. Non viene, invece, punita la negligenza. Vengono sanzionati soltanto coloro che non adottano i provvedimenti minimi per garantire la sicurezza dei dati.

Sono puniti, solo su richiesta, l'inosservanza degli obblighi di informazione, di notifica nonché la violazione degli obblighi di diligenza e dell'obbligo del segreto.

[Il presente promemoria e i suoi allegati sono stati allestiti nel modo più accurato e completo possibile sulla base delle conoscenze attuali. Tuttavia, non è possibile fornire alcuna garanzia legale in merito.](#)

© OmL TC (CAMsuisse)

Soletta, 14.02.2024