OrTra TC Organisation du Monde du Travail Thérapie Complémentaire

Notice pour les thérapeutes sur le DROIT RÉVISÉ DE LA PROTECTION DES DONNÉES

Situation initiale

La révision totale de la loi sur la protection des données (nLPD) entrera en vigueur le 1er septembre 2023. L'objectif de cette révision était d'aligner le droit y relatif sur le droit européen et de renforcer les droits des personnes concernées en matière d'autodétermination et de transparence. Cette notice présente les principales nouveautés et les mesures à prendre.

Aperçu des principaux changements au 1er septembre 2023:

1. Quiconque traite des données doit tenir un **registre des activités de traitement**.
2. Il doit y avoir une **personne responsable de la protection des données** pour chaque fichier.
3. La protection des données doit être assurée sur le **plan technique**.
4. Quiconque traite des données doit **informer les personnes concernées** et leur fournir des renseignements sur demande.
5. Les données doivent être stockées de manière à pouvoir être reproduites et envoyées de manière utilisable **(«portabilité des données»).**
6. **L'effacement des données** est désormais expressément réglementé: quiconque traite des données doit également les effacer en temps utile.
7. Menace en cas d'infraction intentionnelle: **amende** possible jusqu'à CHF 250'000.-.

Explications

La révision de la protection des données impose de nouvelles obligations qui sont décrites dans cette notice. Les questions fréquemment posées (FAQ) sont traitées dans un document séparé. Les bases légales se trouvent dans la loi fédérale sur la protection des données (LPD) et dans l'ordonnance relative à cette dernière (OPDo) et sont reliées en conséquence.

1. Obligation de tenir un registre des activités de traitement (art. 12 nLPD)

La loi exige désormais qu'un **registre** soit tenu pour chaque activité de traitement et qu'il soit actualisé en permanence. Selon l'art. 24 nOPDo, les entreprises de moins de 250 collaborateurs sont exemptées de cette obligation, sauf si des *données personnelles sensibles sont traitées à grande échelle*. Les données relatives à la santé étant considérées comme particulièrement sensibles, il est vivement recommandé aux thérapeutes de tenir un tel registre, indépendamment de toute obligation légale.

2. Personne responsable de la protection des données

Chaque entreprise doit avoir défini une personne concrète comme **responsable de la protection des données**. Cette personne doit disposer des connaissances techniques nécessaires et avoir accès à tous les fichiers. Les thérapeutes travaillant dans un cabinet individuel sont automatiquement responsables de la protection des données.
Le traitement des données personnelles peut être confié par contrat à un sous-traitant. La responsabilité des données incombe donc à une autre organisation (p. ex. cloud-services pour le stockage des données, comptabilité financière externalisée, fournisseur de logiciels Tarif 590). **Une sous-traitance** doit impérativement faire l'objet d'un contrat et contenir les déclarations de protection des données correspondantes (art. 9 nLPD).

3. Mesures techniques et organisationnelles pour la sécurité des données (art. 8 nLPD)

Les mesures techniques concernent les droits d'accès internes (qui a accès à quelles données) et la protection contre l'extérieur (p. ex. pare-feu, mots de passe). Le but de ces mesures est que seules les personnes qui ont besoin d'accéder aux données personnelles pour accomplir leur travail puissent les consulter.

Si des *données personnelles sont perdues, effacées, modifiées ou rendues accessibles à des tiers (non autorisés) (p. ex. en cas de vol)* et que la violation entraîne un risque élevé de conséquences négatives pour la personne concernée, il convient de le signaler au Préposé fédéral à la protection des données (PFPDT).
Envoi de données à caractère hautement personnel: lors de l'envoi de données personnelles, il convient de prendre les mesures nécessaires (notamment l'envoi crypté) pour qu'aucun tiers non autorisé ne puisse les consulter.

4. Droit d'accès/devoir d'information (art. 25 nLPD)

Lorsque des données sont collectées, il doit exister une **déclaration de protection des données**. Cette dernière doit au moins contenir les coordonnées de la personne responsable, le but du traitement et, le cas échéant, les destinataires des données. Une mention sur le site web ou dans des documents écrits doit indiquer où la déclaration de protection des données peut être consultée/retirée. Le fait que la personne concernée la consulte effectivement ne joue aucun rôle.
Les données personnelles doivent être remises aux personnes concernées qui en font la demande dans un délai de 30 jours. Il convient de s'assurer que les données peuvent être trouvées et remises sous forme électronique à la personne concernée dans le délai imparti (voir 5. Portabilité des données).

5. Portabilité des données (art. 28 nLPD)

Les personnes concernées ont désormais le droit de demander leurs données personnelles dans un format électronique courant ou de les faire transmettre à des tiers. En règle générale, la remise ou la transmission des données personnelles doit être gratuite si elle n'entraîne pas de frais excessifs. Il est courant d'utiliser un «format électronique» qui permet la lecture automatique des données dans un système informatique sous une forme structurée (p. ex. en tant que fichier PDF, EXCEL, XML, etc.). Si les documents ne sont pas classés électroniquement et ne sont disponibles que physiquement, ils doivent être scannés et restitués sous forme de document PDF.

6. Effacement des données (art. 6, al. 4 nLPD)

En vertu du principe de proportionnalité, les traitements de données ne peuvent aller au-delà de **ce qui est nécessaire** pour atteindre le but poursuivi. Ensuite, les données doivent être détruites ou anonymisées. Une conservation trop longue de ces dernières constitue une violation de la protection des données.
Les délais de conservation légaux s'appliquent. En règle générale, les **dossiers des patients** doivent être conservés pendant 20 ans. Les données plus anciennes des patients qui ne sont plus en traitement doivent être effacées.
Les documents relevant du droit du travail doivent être supprimés au plus tard 10 ans après le départ de la personne concernée, les documents qui ne sont plus nécessaires, comme les dossiers de candidature, directement après la fin des rapports de travail.
S'il existe des obligations légales de conservation, la demande de suppression ne peut pas être satisfaite.

7. Infractions / sanctions

En cas d'action ou d'omission intentionnelle (délibérée), une amende pouvant atteindre 250'000 CHF peut être infligée, et ce en tant que personne privée. En revanche, la négligence n'est pas sanctionnée. Ne sont donc sanctionnés que ceux qui ne prennent pas les mesures minimales pour assurer la sécurité des données.
Ne sont punis que sur plainte le non-respect des obligations d'information, de renseignement et de déclaration ainsi que le non-respect des obligations de diligence et du secret professionnel.

La présente fiche d'information et ses annexes ont été rédigées de manière aussi précise et complète que possible, en fonction de l'état actuel des connaissances. Néanmoins, aucune garantie juridique ne peut être donnée à ce sujet.

Soleure, le 17.07.2023