Berne, en mai 2023

Droit révisé sur la protection des données - nouveautés et recommandations

Situation de départ

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

Obligation de tenir un registre de tous les traitements de données personnelles

Lors de chaque collecte de données personnelles, les personnes concernées doivent en être informées ; dans le meilleur des cas, on obtient les données d'elles-mêmes et on a donc leur consentement.
La loi exige désormais qu'un registre de chaque activité de traitement soit tenu et mis à jour en permanence. Le registre doit contenir au moins les éléments suivants : Qui est le responsable dans l'entreprise, quel est le but du traitement, les catégories de données, la durée de conservation, les mesures pour garantir la sécurité des données. La loi ne définit pas la forme d'un tel registre.
Il est déconseillé de transférer des données à l'étranger (par ex. stockage de données sur un serveur étranger), sinon des dispositions plus strictes s'appliquent.

Suppression des données

En vertu du principe de proportionnalité, le traitement des données ne doit pas aller au-delà de ce qui est nécessaire pour atteindre le but poursuivi. Ensuite, les données doivent être effacées ou rendues anonymes. Ce qui était valable jusqu'à présent est désormais expressément réglé dans la loi et passible d'une amende : une conservation trop longue des données 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 10 ans. S'il existe des données plus anciennes concernant des patients* qui ne sont plus en traitement, elles doivent être effacées.
Les documents relevant du droit du travail doivent être supprimés au plus tard 10 ans après le départ, les documents qui ne sont plus nécessaires, comme les dossiers de candidature, directement après la fin des rapports de travail.

Sécurité des données

La loi révisée exige que des mesures techniques et organisationnelles soient prises pour assurer une sécurité appropriée des données. Désormais, les violations de la sécurité des données doivent être annoncées au PFPDT lorsqu'elles sont susceptibles d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Il y a violation de la sécurité des données lorsque des données personnelles sont perdues, effacées, modifiées ou rendues accessibles à des tiers (personnes non autorisées). Une notification ne doit être faite que si la violation entraîne un risque élevé de conséquences négatives pour la personne concernée.

Droit à la portabilité des données

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 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. sous forme de fichier EXCEL, XML, etc.).

OdA ARTECURA
Rainweg 9H, 3068 Utzigen
071 330 01 00, info@artecura.ch, www.artecura.ch

Recommandations pour la **mise en œuvre**

- Déclaration de protection des données : lorsque des données sont collectées, une déclaration de protection des données doit exister. Une mention sur le site web ou dans des documents écrits doit indiquer où la déclaration de protection des données peut être consultée/obtenue. Le fait que la personne concernée la consulte effectivement n'a aucune importance. Vous trouverez un modèle de déclaration de protection des données ici : https://www.approoved.com/fr/declaration-de-protection-de-donnees/.
  - ⇒ Sur le site web, il n'est pas nécessaire qu'une fenêtre s'affiche avec une déclaration sur les cookies, mais il doit y avoir un lien visible vers la déclaration de protection des données.
  - ⇒ Pour l'engagement de collaborateurs, la déclaration de protection des données doit être mentionnée dans le contrat de travail ou le règlement du personnel.

- 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.
  - ⇒ Une personne interne ou externe doit être désignée et un cahier des charges doit être établi pour la personne responsable de la protection des données. Vous trouverez un modèle ici : https://www.curaviva.ch/Informations-specialisees/Protection-des-donnees-et-traitement-des-dossiers/PXaEp/?lang=fr.

- Mesures techniques et organisationnelles pour la sécurité des données : sur le plan technique, il s'agit des droits d'accès internes (qui a accès à quelles données) et de la protection contre l'extérieur (pare-feu).
  Sur le plan organisationnel, des instructions et des formations pour le personnel peuvent être utiles.
  Le but de ces mesures est que seules les personnes qui ont besoin d'accéder aux données personnelles pour accomplir leur travail puissent le faire.
  - ⇒ Les personnes travaillant dans un centre de soins ne doivent pas avoir accès aux données de tous les patients, mais uniquement à celles des patients dont elles s'occupent.

- Registre de traitement des données : Quiconque traite des données doit tenir un registre sur la manière dont les données sont traitées. Les informations minimales mentionnées ci-dessus doivent y figurer et être tenues à jour.
  - ⇒ Un document Excel ou Word contenant les données essentielles suffit. Comme but de traitement, il suffit par exemple de mentionner "saisie du temps de travail", "décompte de salaire", "suivi de la clientèle", comme catégories de données personnelles, une désignation telle que "données de contact" ou "temps de travail" suffit et comme catégories de personnes concernées, par exemple "collaborateur", "client".

- Envoi de données à caractère hautement personnel : Lors de l'envoi de données personnelles, des mesures doivent être prises pour qu'aucun tiers non autorisé ne puisse les consulter.
  - ⇒ Si les données personnelles sont envoyées par e-mail, il convient d'utiliser un système qui procède au cryptage (p. ex. HIN).

- Droit à l'effacement : si les personnes concernées demandent l'effacement des données les concernant, celui-ci doit être effectué (sauf pour les données nécessaires, par exemple pour les certificats de travail ou les décomptes).
  Il faut également définir un processus d'effacement des données collectées, en fixant des délais de conservation par catégorie de données.
  - ⇒ La date de création et la durée de conservation correspondante sont affichées de manière bien visible sur chaque document et il est vérifié périodiquement si des suppressions doivent être effectuées.

- Droit d'accès : les données personnelles doivent être communiquées aux personnes concernées dans un délai de 30 jours. Il faut s'assurer que les données puissent être trouvées dans le délai imparti et qu'elles puissent être remises à la personne concernée sous forme électronique.
  - ⇒ Le système de documents doit pouvoir exporter (p. ex. en format PDF).