Berne, mai 2023

Q&R sur le droit révisé de la protection des données

Quels sont les changements les plus fondamentaux au 1er septembre 2023 ?

- Quiconque traite des données doit tenir un registre de traitement
- Pour chaque fichier, il doit y avoir une personne responsable de la protection des données.
- La protection des données doit être assurée par la technique (droits d'accès aux documents, courriers électroniques cryptés)
- Quiconque traite des données doit informer les personnes concernées et leur fournir des renseignements sur demande.
- Les données doivent être stockées de manière à pouvoir être reproduites et transmises ("portabilité des données", par exemple au format PDF ou Excel)
- L'effacement des données est désormais expressément réglementé : quiconque traite des données doit également les effacer en temps utile
- Menace en cas d'infraction intentionnelle : Amende possible jusqu'à 250'000 CHF

La présence d'une personne responsable de la protection des données est-elle obligatoire ?

Dans la loi, il est toujours question de "responsable des données". Il doit donc exister une telle personne pour tous les fichiers, qui en assume la (co)responsabilité et sert d'interlocuteur (également pour les autorités et les tribunaux).

Quelles exigences la personne responsable de la protection des données doit-elle remplir ?

Il n'existe pas de dispositions légales en la matière. La personne doit avoir accès à tous les fichiers/traitements de données et disposer des connaissances spécialisées nécessaires. Par connaissances spécialisées, on entend des connaissances en matière de droit de la protection des données et de technologies de l'information.

Les entreprises de moins de 250 collaborateurs doivent-elles tenir un registre des traitements ?

Selon l'art. 24 nLDP, 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, les thérapeutes* sont tenus de tenir un registre.

Comment les thérapeutes* doivent-ils informer leurs clients ?

La nLPD ne précise pas comment les personnes concernées doivent être informées. Dans la pratique, des déclarations de protection des données sont recommandées, mais une information dans les conditions générales, un formulaire de consentement ou une information orale (par ex. message enregistré) sont également suffisants. En revanche, la simple indication d'une personne de contact pour des questions supplémentaires n'est pas suffisante. Le fait que la personne concernée consulte effectivement la déclaration de confidentialité n'a aucune importance.

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

Que faut-il modifier sur son site web ?
Les personnes concernées doivent désormais être informées du traitement de leurs données. C'est pourquoi une déclaration de protection des données doit être mise en ligne sur le site web et être facile à trouver (mais il n'est pas nécessaire qu'une déclaration de consentement s'affiche).

La déclaration de confidentialité doit-elle être mentionnée sur les cartes de visite, dans les e-mails, etc.
Dans la mesure où la déclaration de protection des données est facilement accessible et reconnaissable sur le site web, il n'est pas nécessaire d'attirer l'attention sur la déclaration de protection des données dans des situations quotidiennes, par exemple lors d'une prise de rendez-vous au guichet ou par e-mail. En effet, on peut raisonnablement attendre de la personne concernée qu'elle consulte la déclaration de confidentialité sur le site web.

Les travailleurs doivent-ils être informés ?
L'article 328b CO constitue une base légale pour le traitement des données des employés. Il est néanmoins recommandé de mentionner explicitement la déclaration de protection des données dans le contrat de travail ou le règlement du personnel.

Quand la transmission à des tiers est-elle autorisée ?
Pour autant que le traitement des données soit licite, qu'il respecte les principes de la protection des données et que les personnes concernées soient informées de la transmission.

Les factures, rapports, etc. peuvent-ils être envoyés par e-mail aux clients/assurances maladie ?
Il convient ici de prendre des mesures techniques afin qu'aucun tiers non autorisé ne puisse consulter les données. Cela peut être réalisé par exemple par un cryptage (p. ex. avec HIN-Mail). En ce qui concerne les données hautement personnelles, il convient de toujours disposer d'un accord explicite ou, mieux encore, de procéder au transfert via la personne concernée.

Quand faut-il annoncer au PFPDT les violations de la sécurité des données ?
Il y a violation lorsque la confidentialité, l'intégrité ou la disponibilité de données personnelles est compromise, c'est-à-dire lorsque des données personnelles sont effacées, perdues, modifiées ou divulguées ou rendues accessibles à des personnes non autorisées. Toutefois, seules les violations qui présentent un risque élevé de conséquences négatives pour les personnes concernées doivent être notifiées.

Que dois-je faire si j'envoie un e-mail au mauvais destinataire ou si je perds une clé contenant des données ?
Il est nécessaire d'évaluer au cas par cas si une communication au PFPDT est nécessaire. Si, par exemple, un courriel contenant des données personnelles est envoyé par erreur à une personne digne de confiance et connue de l'expéditeur*, le risque n'est pas élevé. En revanche, si une clé contenant des données de collaborateurs et leurs salaires est perdue, une déclaration est nécessaire.

Quelles sont les conséquences d'un non-respect des nouvelles règles ?
En cas d'action ou d'omission intentionnelle (délibérée), une amende pouvant aller jusqu'à 250 000 CHF est encourue, et ce en tant que personne privée. La négligence n'est en revanche pas sanctionnée. Ne sont donc sanctionnés que ceux qui ne prennent pas les mesures minimales pour assurer la sécurité des données. Exceptionnellement, l'entreprise peut être amendée jusqu'à CHF 50'000.00 si l'identification de la personne physique implique des efforts disproportionnés.
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 de la déontologie professionnelle.