Association faîtière
des fondations
d'utilité publique
de Suisse

Quels documents doivent être établis conformément à la nouvelle loi sur la protection des données ?

La révision totale de la loi sur la protection des données a été adoptée le 25 septembre 2020 par les Chambres fédérales après de longues tergiversations. Actuellement, l'ordonnance est encore en cours d'élaboration. La nouvelle loi sur la protection des données (nLPD) devrait finalement entrer en vigueur le 1er septembre 2023. Cette date est très importante pour tous ceux qui traitent des données, car aucun délai de transition n'est prévu pour la mise en œuvre des dispositions légales. Lors de l'entrée en vigueur, toutes les dispositions légales devront donc déjà être mises en œuvre. Vous trouverez ci-dessous un aperçu des documents les plus importants.

1. Documents requis par la loi

1.1. La déclaration de protection des données (respect de l'obligation d'information)

Il n'est pas expressément exigé par la loi de rédiger d'une déclaration de protection des données, mais c'est le moyen le plus simple de satisfaire à l'obligation d'information prescrite par la loi. Selon l'article 19 nLPD, le responsable du traitement des données doit en effet informer de manière adéquate la personne dont les données sont traitées sur la collecte des données personnelles. Ce devoir d'information s'applique également lorsque les données ne sont pas collectées auprès de la personne concernée.

Lors de la collecte, il convient de communiquer à la personne concernée les informations nécessaires pour qu'elle puisse faire valoir ses droits et garantir un traitement transparent des données.

La déclaration de protection des données informe la personne concernée, d'une part, sur le traitement des données en soi et, d'autre part, sur les droits qui lui sont conférés par la loi sur la protection des données. Il convient de respecter les exigences légales minimales selon l'art. 19, al. 2 nLPD. Ainsi, l'identité et les coordonnées du responsable ainsi que le but du traitement doivent être indiqués. Le cas échéant, les destinataires ou les catégories de destinataires auxquels les données personnelles sont communiquées doivent être mentionnés.

Étant donné qu'il est très important de présenter l'ensemble du traitement des données de manière claire et transparente et d'indiquer également clairement la finalité du traitement, une déclaration de protection des données doit correspondre au traitement effectif des données. Il est donc recommandé de vérifier précisément ce qu'il faut comme informations dans la déclaration de protection des données. Nous vous recommandons donc de vous faire conseiller par un expert en la matière. proFonds vous renseignera volontiers et vous mettra en contact avec un expert.

1.2. L'analyse d'impact sur la protection des données

L'analyse d'impact relative à la protection des données (art. 22 nLPD) est un instrument de gestion préventive des risques. Il s'agit donc d'un document qui doit permettre d'estimer si le traitement de données prévu pourrait présenter un risque.

Le responsable doit identifier au préalable les risques résultant de son traitement et définir des contre-mesures appropriées si un traitement est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées. L'existence d'un risque élevé doit être vérifiée au cas par cas et dépend de différents facteurs (type de données traitées, volume et durée du traitement des données).

Le risque élevé résulte, notamment en cas d'utilisation de nouvelles technologies, de la nature, de l'ampleur, des circonstances et de la finalité du traitement. Un tel risque doit notamment être supposé lorsque des données sensibles sont traitées à grande échelle ou que des domaines publics étendus sont systématiquement surveillés. Les données sensibles sont par exemple les données relatives aux opinions religieuses, philosophiques, politiques ou syndicales, les données relatives à la santé, à la sphère intime ou à l'appartenance à une race ou une ethnie, les données génétiques, les données biométriques, les données relatives aux poursuites ou sanctions administratives et pénales ainsi que les données relatives aux mesures d'aide sociale.

L'analyse d'impact relative à la protection des données contient une description du traitement prévu, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée ainsi que les mesures prises pour protéger la personnalité et les droits fondamentaux.

1.3. Le registre de traitement

Conformément à l'article 12 de la nLPD, le responsable du traitement et tous les sous-traitants sont tenus de tenir un registre de leurs activités de traitement.

Le registre de traitement est une description générale des activités de traitement et non une liste de traitements de données concrets. Ici aussi, la loi fixe des exigences minimales.

Les entreprises qui emploient moins de 250 personnes et dont le traitement des données présente un faible risque d'atteinte à la personnalité des personnes concernées n'ont pas l'obligation de tenir un registre de traitement. Selon le P-OLPD, on peut considérer qu'un tel traitement de données présente des risques minimes s'il ne porte pas sur un grand nombre de données personnelles sensibles et s'il ne comporte pas de profilage à haut risque (pour les droits fondamentaux de la personne concernée). On parle d'un tel risque élevé lorsqu'il y a une mise en relation de données qui permet d'évaluer des aspects essentiels de la personnalité d'une personne physique.

2. Directives selon l'ordonnance

2.1 Le règlement de traitement

La nLPD ne prévoit pas l'obligation d'établir un règlement de traitement. Mais telle obligation est prévue au niveau de l'ordonnance (art. 4 P-OLPD).

Selon celle-ci, le responsable du traitement ainsi que tous les sous-traitants doivent établir un règlement pour les traitements automatisés lorsqu'ils traitent un grand nombre de données personnelles sensibles ou lorsqu'ils effectuent un profilage à haut risque.

Le règlement doit contenir au moins les indications suivantes : le but du traitement ; les catégories de personnes concernées, les catégories de données personnelles traitées, la durée de conservation des données personnelles ou les critères de détermination de cette durée, l'origine des données personnelles, le mode de collecte, les mesures techniques et organisationnelles visant à garantir la sécurité des données, les autorisations d'accès, le type et l'étendue des accès, les mesures visant à minimiser les données, les procédures de traitement des données, notamment les procédures d'enregistrement, de rectification, de communication, de conservation, d'archivage, de pseudonymisation, d'anonymisation et d'effacement ou de destruction, les procédures d'exercice du droit d'accès et du droit de remise ou de transmission des données.

On ne sait pas encore si l'obligation de tenir un règlement de traitement restera dans l'ordonnance malgré l'absence de base légale.

3. Documents recommandés

3.1. Le formulaire de renseignements

Conformément à l'article 25 de la nLPD, toute personne concernée peut demander au responsable du traitement si des données personnelles la concernant sont traitées. La personne concernée reçoit les informations nécessaires pour qu'elle puisse faire valoir ses droits conformément à la présente loi et pour garantir un traitement transparent des données. La loi définit à l'article 25, alinéa 2 nLPD quelles informations doivent être communiquées dans quel cas.

Même si un formulaire de renseignements n'est pas prescrit par la loi, il est recommandé d'en établir un afin de permettre des processus internes plus efficaces grâce à des communications de renseignements standardisées.

3.2. Contrat de traitement sur mandat Garantir une protection des données adéquate

Conformément à l'article 9 nLPD, le traitement de données personnelles peut être confié à un sous-traitant (traitement sur mandat). Si le traitement des données est délégué à un tiers, le responsable qui confie le traitement des données personnelles au sous-traitant reste responsable de la protection des données. Pour cette raison, un traitement sur mandat ne peut être effectué que si les données sont traitées comme le responsable pourrait le faire lui-même et si aucune obligation légale ou contractuelle de confidentialité n'interdit la délégation.

Le responsable doit notamment s'assurer que le sous-traitant est en mesure de garantir la sécurité des données. Il doit en outre s'assurer que le sous-traitant est soumis à la LPD ou à une loi étrangère garantissant une protection des données équivalente. Si ce n'est pas le cas, le responsable doit assurer la protection des données en rédigeant le contrat (fourniture de garanties ou utilisation de clauses contractuelles standard).

L'annexe 1 de la P-OLPD contient une liste d'Etats qui garantissent une protection adéquate des données. Cette liste est revue périodiquement. Les pays qui ne garantissent pas une protection adéquate des données sont supprimés. Pour les responsables qui délèguent le traitement de leurs données à un tiers ayant son siège à l'étranger, il est recommandé de contrôler régulièrement cette liste.

Nous nous tenons à votre disposition pour tout complément d'information.

proFonds, Association faîtière des fondations d'utilité publique

061 272 10 80
info@proFonds.org
www.proFonds.org