Check-list : mise en œuvre de la nouvelle protection des données

Les explications suivantes portent sur les principales tâches nécessaires à la mise en œuvre de la nouvelle loi suisse sur la protection des données (nLPD), qui entrera en vigueur le 1er septembre 2023. L'accent est mis sur les points qui sont principalement pertinents pour les membres de l'ASSL et de l'UPSA. Il n'existe pas de solution à « taille unique ». Chaque cas doit être considéré séparément. Cette check-list ne prétend donc pas être exhaustive.

- Définir les **responsabilités et les fonctions pour la planification du projet** dans le cadre de la mise en œuvre des nouvelles règles de protection des données.
- Établir un **registre des traitements de données à caractère personnel** (« registre de traitement »), comme dans les domaines du marketing, des ressources humaines, de l'exécution des contrats, etc. Il s'agit d'une obligation légale si votre entreprise compte plus de 250 collaborateurs, traite des données personnelles sensibles à grande échelle ou effectue un profilage à risque élevé (art. 12 nLPD et art. 24 OLPD). Dans les autres cas, le registre peut être établi sur une base volontaire et servir de base à l'exécution d'autres obligations, telles que les devoirs d'informer vis-à-vis des personnes concernées.
- Vérifier si un **conseiller à la protection des données** doit ou devrait être nommé (contrairement au RGPD, c'est facultatif pour les particuliers selon la nLPD – seuls les organes fédéraux y sont légalement tenus, art. 10 nLPD).
- Rédaction de **déclarations de protection des données** pour le site web, pour les activités de l'entreprise et pour les collaborateurs (ainsi que les candidats), afin d'assumer les devoirs d'informer envers les personnes concernées (art. 19 nLPD et art. 13 OLPD).
- Vérification et mise à jour des mesures relatives à **la sécurité des données** (art. 8 nLPD et art. 1 ss OLPD) ; en particulier, mesures techniques et organisationnelles de sécurité des données (art. 3 OLPD) ; procès-verbaux de journalisation (art. 4 OLPD) et établissement d'un règlement de traitement pour les traitements automatisés de données (art. 5 s. OLPD).
- Élaboration de **règlements et de processus pour le respect des droits des personnes concernées** ; en particulier pour l'annonce des violations de la protection des données (art. 24 nLPD et art. 15 OLPD), la conservation et l'effacement des données (art. 6, ch. 4 nLPD), le droit d'accès (art. 25 nLPD et art. 16 ss OLPD) et le droit à la portabilité des données (art. 28 nLPD et art. 20 ss OLPD).
- Vérification et mise à jour des **contrats de traitement des données avec des tiers** (art. 9 nLPD et art. 7 OLPD), notamment en ce qui concerne les communications de données à l'étranger (art. 16 nLPD et art. 8 ss OLPD). Examiner et actualiser les accords de transfert de données internes à des groupes, le cas échéant.

- Examiner et mettre à jour d'autres accords (avec des clients, des fournisseurs, des collaborateurs, etc.) en ce qui concerne les aspects liés à la protection des données.
- Réaliser des **analyses d'impact relatives à la protection des données** lorsqu'un traitement est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 22 s. nLPD et art. 14 OLPD).
- Définir et mettre en œuvre des **formations** pour les collaborateurs. Cela n'est certes pas explicitement exigé par le RGPD ni par la nLPD, mais s'avère souvent nécessaire pour créer la sensibilité nécessaire à ce sujet au sein de l'entreprise. Les formations peuvent être organisées par l'entreprise elle-même ou par des personnes externes, comme l'ASSL, en collaboration avec l'UPSA Business Academy. Vous trouverez nos offres à l'adresse : webinaire LPD.
- Définir des **procédures et des responsabilités pour vérifier et mettre à jour régulièrement** la conformité en matière de protection des données.

***

Septembre 2022