Check-list : Mise en œuvre de la nouvelle loi sur la protection des données

Les explications suivantes portent sur les principales mesures 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. Dans ce contexte, il n'existe pas de solution unique, mais chaque cas doit être considéré individuellement. La check-list ci-dessous est fournie à titre informatif et ne prétend pas être exhaustive.

- Définir les **responsabilités et les fonctions pour la planification du projet** de mise en œuvre des nouvelles règles de protection des données.
- Établir un **registre des traitements de données personnelles** (appelé registre de traitement), comme par exemple dans les domaines du marketing, des RH, 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 haut risque (art. 12 nLPD et art. 24 OPDo). Dans les autres cas, le registre peut être établi volontairement et servir de base pour remplir d'autres obligations, telles que les obligations d'information envers les personnes concernées.
- Vérifier si un **conseiller à la protection des données** doit ou devrait être nommé (contrairement au RGPD, sous la nLPD, cela est facultatif pour les particuliers - seuls les organes fédéraux y sont légalement tenus, art. 10 nLPD).
- Rédaction de **déclarations de protection des données** pour le site internet, pour les activités de l'entreprise et pour les collaborateurs (ainsi que les candidats), afin de se conformer aux obligations d'information envers les personnes concernées (art. 19 nLPD et art. 13 OPDo).
- Vérification et mise à jour des mesures relatives à **la sécurité des données** (art. 8 nLPD et art. 1 ss OPDo) ; en particulier, mesures techniques et organisationnelles de sécurité des données (art. 3 OPDo) ; journalisation (art. 4 OPDo) et établissement d'un règlement de traitement pour les traitements automatisés de données (art. 5 s. OPDo).
- Création de **règlements et de processus pour le respect des droits des personnes concernées** ; en particulier pour la notification des violations de la protection des données (art. 24 nLPD et art. 15 OPDo), la conservation et l'effacement des données (art. 6, ch. 4 nLPD), le droit d'accès (art. 25 nLPD et art. 16 ss OPDo) et le droit à la portabilité des données (art. 28 nLPD et art. 20 ss OPDo).
- Vérification et mise à jour des **contrats de traitement des données avec des tiers** (art. 9 nLPD et art. 7 OPDo), notamment en ce qui concerne les tranferts transfrontaliers (art. 16 nLPD et art. 8 ss OPDo). Le cas échéant, vérification et mise à jour des accords de transfert de données au sein du groupe.
- Examiner et mettre à jour d'autres contrats (avec des clients, des fournisseurs, des employés, etc.) pour les aspects liés à la protection des données.
- Réaliser des **analyses d'impact sur la protection des données** lorsqu'un traitement peut entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 22 s. nLPD et art. 14 OPDo).
- Définir et organiser des **formations** pour les collaborateurs. Cela n'est certes pas explicitement exigé par le RGPD ni par la nLPD, mais est essentiel pour sensibiliser l’ensemble du personnel de l'entreprise.
- Définir des **procédures et des responsabilités pour vérifier et mettre à jour régulièrement** la conformité en matière de protection des données.