Entrée en vigueur au 1er septembre 2023

Nouvelle loi sur la protection des données

Entamé en 2010, le processus législatif pour réviser la loi sur la protection des données (LPD) a pris du temps. La loi a finalement été adoptée en septembre 2020 et entrera en vigueur au 1er septembre 2023. Elle poursuit deux buts : premièrement, la loi actuelle doit être adaptée à l'environnement numérique. Deuxièmement, elle doit se rapprocher de la législation européenne. Au vu de la durée du processus législatif, aucune période de transition n'est prévue. C'est donc dès à présent que les entreprises doivent préparer le changement. Explications sur ce qui change – et sur ce qui reste pareil.

Martina Guillod

Le présent article traite de la loi fédérale sur la protection des données (LPD), applicable aux traitements de données par les entreprises privées. Il faut toutefois savoir que chaque canton a sa propre loi sur la protection des données, applicable aux traitements faits par le canton ou les communes, et qui sera révisée selon le planning cantonal.

Il se peut aussi que certaines entreprises soient déjà soumises au règlement européen sur la protection des données (RGPD), entré en vigueur en mai 2018 dans l'Union européenne (UE). Tel est le cas des entreprises qui ciblent des consommateurs dans l'Union européenne pour leur offrir des services (par exemple via un commerce en ligne) ou qui ciblent leur comportement dans l'UE. Pour les entreprises qui sont déjà conformes au RGPD, la nouvelle LPD n'apportera pas de changement majeur.

Ce qui reste inchangé

Les grands principes de la protection des données ne seront pas modifiés. Ils sont au nombre de six : La bonne foi, l'obligation de traiter le moins de données possibles pour le but visé (proportionnalité), l'obligation d'informer sur le traitement des données (information), l'obligation de ne traiter que des données exactes et de corriger des données erronées (exactitude), l'obligation de n'utiliser les données collectées que pour le but pour lequel elles ont été collectées (finalité) et l'obligation de traiter les données de manière sécurisée (sécurité).

Le traitement des données est légal si aucun des principes ci-dessus n'est violé, si la personne concernée ne s'oppose pas expressément au traitement et s'il ne s'agit pas de données sensibles transmises à un tiers. Si ces conditions ne sont pas remplies, la personne souhaitant traiter les données doit avoir un motif justificatif (loi, intérêt prépondérant ou consentement de la personne concernée), faute de quoi le traitement n'est pas possible.

Nouveautés

- **Privacy by design et privacy by default :** Dès la conception d'un produit ou d'un service, l'entreprise doit prendre les mesures appropriées pour que celui-ci respecte la LPD. Les données doivent être protégées automatiquement grâce à un paramétrage par défaut, sans que l'utilisateur ait à l'activer.

- **Registre des activités de traitement :** Les entreprises doivent tenir un document interne qui détaille notamment les catégories de données traitées, les personnes concernées, la finalité du traitement, les catégories de destinataires, le délai de conservation des données personnelles et les mesures de sécurité prises. Les entreprises privées employant moins de 250 personnes sont exemptées de cette obligation, sauf si le traitement porte sur des données sensibles à grande échelle (par exemple dans un cabinet médical) ou s'il constitue un profilage à risque élevé.

- **Le devoir d'informer :** La personne qui traite les données doit informer sur l'identité et les coordonnées du responsable de traitement, sur la finalité du traitement et, le cas échéant, sur les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises. En cas de communication transfrontalière des données (dont l'enregistrement de données sur un cloud fait partie), le responsable du traitement doit informer sur le pays de destination et le niveau de protection offert. Ces informations peuvent par exemple figurer sur le site internet de l'entreprise. Jusqu'à présent, cette obligation ne valait que pour le traitement des données sensibles. Elle est dorénavant applicable à toutes les données personnelles.

- **Le devoir d'informer en cas de décisions individuelles automatisées :** La personne concernée doit être informée si une décision à son égard a été prise sur la base d'un algorithme seulement, sans aucune contribution humaine. Elle a ensuite le droit de faire revoir la décision par une personne physique.

- **Analyse d'impact :** En présence d'un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (par exemple en cas de traitement de données sensibles à grande échelle), le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. L'analyse doit évaluer les risques et proposer des mesures de protection.

- **Annonce des violations de sécurité :** Les violations de la sécurité des données qui entraînent vraisemblablement un risque élevé pour la personnalité concernée doivent être annoncées au préposé fédéral à la protection des données et à la transparence (PFPDT).

- **Le droit à la portabilité :** Ce droit permet à la personne concernée de demander au responsable de traitement que les données informatiques qu'elle lui a communiquées lui soient remises dans un format électronique couramment utilisé.

- **Sanctions :** Le PFPDT doit dorénavant ouvrir une enquête d'office s'il constate un traitement de données contraire à la législation ; en revanche, il ne dispose pas du pouvoir d'infliger des amendes administratives. Au niveau pénal, la LPD prévoit des amendes jusqu'à 250 000 francs en cas d'infraction intentionnelle. Il est important de noter que c'est en principe la personne physique qui sera responsable. L'entreprise ne sera punie que si l'identification de la personne responsable nécessite des mesures d'enquête disproportionnées.