Nouvelle loi sur la protection des données (nLPD)

La Suisse se dote d'une nouvelle législation pour mieux protéger les données personnelles. Les entreprises du pays doivent s'y conformer à partir du 1er septembre 2023.

Lors de sa session d'automne 2020, le Parlement a adopté la nouvelle la loi fédérale sur la protection des données (nLPD). Elle améliore le traitement des données personnelles et accorde de nouveaux droits aux personnes concernées. Ce changement législatif important s'accompagne également d'un certain nombre d'obligations pour les entreprises.

La loi sur la protection des données, totalement révisée, et les dispositions d'exécution inscrites dans les nouvelles ordonnances sur la protection des données (OPDo) et sur les certifications en matière de protection des données (OCPD) entreront en vigueur le 1er septembre 2023.

Une nouvelle loi nécessaire

La première loi fédérale sur la protection des données date de 1992. Entre temps, la population suisse a introduit l'usage d'Internet et des smartphones dans son quotidien; et a toujours plus recours aux réseaux sociaux, au Cloud ou à l'internet des objets. Dans ce contexte, un remaniement complet de la loi sur la protection des données – et plus seulement partiel comme en 2009 et 2019 –, est indispensable pour assurer à la population une protection de ses données adéquate et adaptée aux évolutions technologiques et sociales de notre époque.

La compatibilité du droit suisse avec le droit européen, et notamment le Règlement européen sur la protection des données (RGPD), constitue l'autre enjeu principal de la nouvelle loi. La nLPD devrait permettre de maintenir la libre circulation des données avec l'Union européenne (UE) et ainsi d'éviter une perte de compétitivité des entreprises suisses.

Quels sont les principaux changements?

La nLPD introduit les huit changements majeurs suivants pour les entreprises.

1. **Seules les données des personnes physiques** sont dorénavant couvertes, et non plus celles des personnes morales.
2. **Les données génétiques et biométriques** entrent dans la définition des données sensibles.
3. **Les principes de "Privacy by Design" et de "Privacy by Default"** sont introduits. Comme son nom l'indique, le principe de "Privacy by Design" (protection des données dès la conception) implique, pour les développeurs, d'intégrer la protection et le respect de la vie privé des utilisateurs dans la structure même du produit ou du service amené à collecter des données personnelles. Le principe de "Privacy by Default" (protection des données par défaut) assure quant à lui le niveau de sécurité le plus élevé dès la mise en circulation du produit ou du service, en activant par défaut, c'est-à-dire sans aucune intervention des utilisateurs, toutes les mesures nécessaires à la protection des données et à la limitation de leur utilisation. Autrement dit, tous les logiciels, le matériel et les services doivent être configurés de manière à protéger les données et à respecter la vie privée des utilisateurs.
4. **Des analyses d'impacts** doivent être menées, en cas de risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.
5. **Le devoir d'informer** est étendu: la collecte de toutes les données personnelles – et non plus uniquement de données dites sensibles –, doit donner lieu à une information préalable de la personne concernée.
6. **La tenue d'un registre des activités de traitement** devient obligatoire. L'ordonnance d'application prévoit toutefois une exemption pour les PME dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées.
7. **Une annonce rapide** est requise en cas de violation de la sécurité des données, à adresser au Préposé fédéral à la protection des données et à la transparence (PFPDT).
8. **La notion de profilage** (soit le traitement automatisé de données personnelles) fait son entrée dans la loi.

Le site du PFPDT (Nouvelle loi fédérale sur la protection des données) offre des informations plus précises et détaillées concernant les modifications apportées par la nLPD.

Différences avec l'UE

Les entreprises qui s'étaient déjà conformées au règlement général de l'UE sur la protection des données (RGPD) auront peu de changements à entreprendre. L'association SwissPrivacy.Law a publié un tableau de comparaison entre la nLPD et le règlement européen à consulter à cette adresse (en français): https://swissprivacy.law/55/

Informations

Liens | En discussion

La nouvelle loi sur la protection des données (LPD)

Renforcement de la protection des données

Réglementation UE pour la protection des données

Was das neue Datenschutzgesetz bewirkt

Netzwoche: Interview mit Adrian Lobsiger, EDÖB

Datenschutz auf dem neuesten Stand - KMU-Praxisratgeber

(gryps.ch) en allemand

Dernière modification 07.11.2023

Début de la page