Loi Suisse sur la Protection des Données personnelles (nLPD)

Document explicatif sur la loi et sa mise en œuvre

Contexte et historique :

La législation fédérale en matière de protection des données, qui datait de 1992 (voir l'ordonnance de 1993), a été adaptée aux développements technologiques. Cette révision est importante pour que la Suisse continue à être reconnue par l'UE comme un État tiers ayant un niveau de protection des données **adéquat** et que l'échange de données transfrontière demeure possible.

Le Parlement a adopté la nouvelle loi sur la protection des données (nLPD) lors de sa session d'automne 2020. En vue de son entrée en vigueur, l'ordonnance relative à la loi sur la protection des données (OLPD) a dû être adaptée. Le Conseil fédéral a ouvert la procédure de consultation à l'occasion de la séance du 23 juin 2021 (Révision de l'ordonnance) qui s'est achevée le 14 octobre 2021 (https://www.kmu.admin.ch/kmu/fr/home/faits-et-tendances/digitalisation/protection-des-donnees/nouvelle-loi-sur-la-protection-des-donnees-nlpd.html)

Le 31 août 2022 le Conseil fédéral annonce officiellement que le nouveau droit de la protection des données entrera bien en vigueur le 1er septembre 2023.

https://www.admin.ch/gov/fr/accueil/documentation/communiques/communiques-conseil-federal.msg-id-90134.html

Comparatif entre la loi de 1992 (OLPD) et la nouvelle nLPD
https://www.newsd.admin.ch/newsd/message/attachments/75615.pdf

Ordonnance :

L'ordonnance a été publiée le 31 août 2022 et est disponible ici :
https://www.fedlex.admin.ch/eli/oc/2022/568/fr

Entreprises et organisations concernées :

Toute société ou organisation qui collecte, traite ou stocke des données personnelles est concernée par la législation sur la protection des données, afin d'assurer la sécurité et la confidentialité des informations individuelles conformément aux exigences légales.

Les nouveautés dans cette révision de la Loi :

Nouvelles obligations

Loi fédérale sur la protection des données (LPD) : (site officiel du texte de loi)

Le devoir d'information, imposé par la législation actuelle en cas de collecte de données sensibles et de profils de la personnalité (art. 14 LPD), est étendu à toutes les données personnelles (art. 19 nLPD). La nLPD impose ainsi au responsable du traitement d'informer la personne concernée de toute collecte de données personnelles (art. 19). Il doit au moins lui communiquer son identité et ses coordonnées, la finalité du traitement et, cas échéant, les destinataires ou catégories de destinataires auxquels les données sont transmises. La nLPD prévoit toutefois des exceptions et restrictions à ce devoir (art. 20).

Le responsable du traitement doit tenir un registre des activités de traitement (art. 12 nLPD). Les entreprises employant moins de 250 collaborateurs devraient toutefois être déliées de cette obligation, à moins que le traitement porte sur des données sensibles à grande échelle ou constitue un profilage à risque élevé (art. 26 p-OPD).

Les principes de protection des données dès la conception et par défaut sont ancrés dans la nLPD (art.7). Le responsable du traitement doit mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions dès la conception du traitement. Il est également tenu de garantir, par le biais de préréglages appropriés, que le traitement soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement.

Une analyse d'impact doit être réalisée au préalable lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux (art. 22 nLPD). Un tel risque existe notamment lors d'un traitement de données sensibles à grande échelle ou de surveillance systématique de grandes parties du domaine public.

En cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux, une annonce doit être effectuée auprès du Préposé fédéral à la protection des données et à la transparence (PFPDT) dans les meilleures délais (art. 24 nLPD). La personne concernée doit également être informée de la violation lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige.

Sous-traitants hors de Suisse selon la nLPD

La nouvelle Loi fédérale sur la protection des données (nLPD), entrée en vigueur le 1er septembre 2023, impose des exigences strictes pour le transfert de données personnelles vers des sous-traitants situés hors de Suisse, y compris vers les pays dits adéquats. Ces exigences sont alignées sur celles du RGPD pour garantir un niveau de protection adéquat des données personnelles.

Pays Adéquats : La Suisse a établi une liste de pays considérés comme offrant un niveau de protection adéquat pour les données personnelles. Cette liste est régulièrement mise à jour par le Préposé fédéral à la protection des données et à la transparence (PFPDT). Les pays de l'UE, l'EEE, ainsi que certains autres pays comme le Canada et Israël, figurent sur cette liste.

Liste des pays dit « Adéquats » :
https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/internationales/anerkennung-staaten.html

Sous-traitance et Transfert de Données :

Contrats de Sous-traitance : Tout transfert de données vers des sous-traitants dans des pays adéquats doit être encadré par un contrat de sous-traitance. Ce contrat doit inclure des clauses types de protection des données, conformément à l'article 16, al. 2, let. d de la nLPD.

Garanties Spécifiques : Des garanties spécifiques doivent être mises en place pour assurer la protection des données personnelles transférées. Ces garanties peuvent inclure des règles d'entreprise contraignantes ou des codes de conduite approuvés.

Obligations du Responsable du Traitement :

Évaluation du Niveau de Protection :

Avant de transférer des données, le responsable du traitement doit évaluer le niveau de protection des données dans le pays de destination (Art. 16, al. 1 nLPD).

Si le pays est jugé adéquat, le transfert peut se faire sous réserve de la mise en place des garanties nécessaires.

Information et Consentement :

Les personnes concernées doivent être informées du transfert de leurs données personnelles à l'étranger, notamment en ce qui concerne la finalité du transfert et les garanties mises en place (Art. 19 nLPD)

Notification au PFPDT :

En cas de transfert vers un pays qui n'est pas reconnu comme offrant un niveau de protection adéquat, le responsable du traitement doit notifier le Préposé fédéral à la protection des données et à la transparence (PFPDT) et obtenir son autorisation préalable (Art. 16, al. 2 nLPD).

Sanctions :

Les droits des individus sont renforcés. La nLPD (art. 25-29) leur accorde un droit d'accès ainsi qu'un droit à la remise ou à la transmission de leurs données (droit à la portabilité). Le PFPDT dispose de pouvoirs d'enquête élargis (accès aux locaux, audition de témoins, etc.). Il peut rendre des décisions contraignantes, par exemple ordonner la cessation du traitement ou interdire la communication de données à l'étranger (art. 50 et 51 nLPD).

En cas de violation intentionnelle de ses obligations, le responsable du traitement peut être condamné à une **amende s'élevant jusqu'à CHF 250'000.-** (art. 60 ss nLPD ; à titre de comparaison, le RGPD prévoit des amendes pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial).

Mise en œuvre de la conformité aux réglementations sur les données personnelles :

Pour se conformer aux exigences légales et minimiser les risques de préjudices financiers ou de dommages à leur réputation, il est crucial d'adopter une série de mesures proactives :

1. **Inventaire des données** : Réaliser un audit complet des données personnelles détenues par l'entreprise pour identifier précisément quelles données sont collectées, stockées, et traitées.
2. **Mise à niveau de la sécurité informatique** : Renforcer les systèmes de sécurité informatique pour protéger les données contre les accès non autorisés, les pertes ou les fuites de données.
3. **Révision des contrats** : Vérifier et ajuster les contrats avec les clients, fournisseurs, et sous-traitants pour garantir qu'ils incluent des clauses de protection des données personnelles conformes aux normes légales.
4. **Politique de confidentialité** : Élaborer ou mettre à jour une politique de confidentialité claire et accessible, détaillant les pratiques de l'entreprise concernant le traitement des données personnelles.
5. **Gestion des cookies** : Mettre en place un système efficace pour informer les utilisateurs et recueillir leur consentement concernant l'utilisation de cookies sur les sites web de l'entreprise.
6. **Suppression régulière des données** : Établir une procédure pour la suppression régulière des données inutiles ou obsolètes pour ne conserver que les données nécessaires.
7. **Procédure en cas d'incident de sécurité** : Développer un protocole d'action rapide en cas de violation ou d'incident de sécurité affectant les données personnelles.
8. **Formation des employés** : Organiser des sessions régulières de sensibilisation et de formation pour les employés sur les meilleures pratiques en matière de protection des données et les obligations légales.

Ces mesures constituent une approche globale et stratégique pour la gestion des risques liés aux données personnelles et pour assurer la conformité avec les réglementations en vigueur.

Accompagnement

Alrix Consulting, grâce à ses consultants expert et DPO certifiés, vous accompagne dans la démarche de mise en conformité et dans la constitution d'une documentation de preuves destinés à vos clients, fournisseurs, sous-traitants et autorité de contrôle.

Voici les principales étapes de cet accompagnement :

1. **Initialisation du Projet** :
    - Signature d'un accord de confidentialité.
    - Sensibilisation des équipes aux données personnelles et à la loi à travers des séances d'information.
2. **Diagnostic et Identification des Non-Conformités** :
    - Réalisation d'un état des lieux pour identifier les écarts de conformité, incluant des interviews des responsables de départements.
    - Remise d'une feuille de route avec des recommandations d'actions à entreprendre auprès de la direction.
3. **Accompagnement à la Mise en Conformité** :
    - Conseils de remédiations pour combler les écarts identifiés.
    - Constitution de la documentation nécessaire (registres, contrats, politique de confidentialité, etc.).
    - Assistance continue pour la mise en place des remédiations et la réponse aux questions des membres de l'organisation.
4. **Suivi en Continu de la Conformité** :
    - Service de DPO (Data Protection Officer) pour gérer les formalités en cas de violation de données et être l'interlocuteur avec les autorités de contrôle.
    - Revue annuelle de conformité pour identifier les modifications nécessaires.
5. **Formation et Sensibilisation** :
    - Séances d'initiation aux enjeux et principes de la protection des données pour créer des réflexes et comprendre les recommandations.
    - Formation continue des équipes pour maintenir un haut niveau de conformité et de sécurité des données.

Alrix Consulting peut également être votre DPO (conseiller à la protection des données) afin de vous assister au quotidien pour toutes les questions ou sollicitations de tiers, tel que exercices de droits, violation de données, contrat de sous-traitance, politiques de confidentialité, etc.

Autres informations sur le site : https://alrix.ch/lpd

Version 1.3 – septembre 2023