Planifier pour mieux protéger: la protection des données et sa mise en œuvre

Le domaine de la protection des données a fortement évolué ces dernières années. L'avènement du RGPD en mai 2018 a bouleversé les pratiques, nécessitant un grand travail d'adaptation du fonctionnement des entreprises. Cette évolution continue en Suisse par l'adoption de la LPD révisée, qui devrait entrer en vigueur en fin d'année 2022. Un travail consciencieux et adapté à chaque société est d'ores et déjà nécessaire afin d'implémenter les nouvelles mesures.

La mise en œuvre de la Loi sur la protection des données révisée (nLPD) et de ses nouveautés nécessite de procéder en plusieurs étapes. Cependant, certaines mesures devront être prises en priorité afin d'éviter de se retrouver en porte-à-faux avec la nouvelle Loi.

Etape zéro: une bonne préparation

Tout d'abord, l'entreprise devra chercher à se positionner vis-à-vis du cadre juridique pertinent, en se posant les questions suivantes:

- Serons-nous soumis à la nLPD?
- Avons-nous déjà implémenté les exigences du RGPD?
- Est-ce que d'autres dispositions sectorielles s'appliquent (par ex. sur la protection des secrets, les assurances maladies, la santé)?
- Est-ce qu'il serait opportun d'appliquer volontairement le RGPD? Le cas échéant, quel serait l'impact de cette application volontaire sur notre mise en œuvre de la nLPD?

Le registre des activités de traitement, un élément de clarté

Il permet d'enregistrer toutes les activités de traitement effectuées par le responsable de traitement et sous-traitant. Des processus adéquats d'enregistrement des activités de traitement devront être mis en place pour en assurer un fonctionnement optimal. En outre, les registres déjà créés sous le RGPD devront être adaptés à la nLPD.

Un fonctionnement interne efficace

Les entreprises doivent bénéficier d'une structure adéquate et des compétences nécessaires pour respecter les obligations de la nLPD. Il est donc recommandé de:

- documenter les traitements;
- avoir un personnel formé;
- adopter des lignes directrices, politiques internes et notices d'information ou adapter celles développées sous le RGPD.

Il peut également être opportun de nommer un conseiller à la protection des données.

Un devoir d'information général actif

La nLPD impose un devoir d'information à chaque collecte de données personnelles. Il sera alors nécessaire de vérifier lors de la collecte:

- l'origine et la manière dont les données sont obtenues;
- les outils utilisés pour informer les personnes concernées de la protection des données (par ex. dans les politiques de confidentialité);
- si et quand le consentement est utile, voire obligatoire;
- la forme que peut prendre le consentement.

> **Une mise en œuvre réussie et durable de la nouvelle Loi sur la protection des données n'est pas obligatoirement compliquée et coûteuse, mais laisse au contraire une certaine marge de manœuvre.**

La conclusion de nouveaux contrats et la revue des contrats existants

Si ce n'est pas déjà le cas, les entreprises devront conclure des contrats notamment avec les fournisseurs, les clients et les sous-traitants afin de définir les responsabilités et obligations de chacun en matière de protection des données. Les contrats existants devront également faire l'objet d'une revue.

Privacy by design, by default et la sécurité des données

Les entreprises doivent veiller à ce que:

- les traitements des données soient conformes aux exigences de la protection des données dès la conception (*privacy by design*) et par défaut (*privacy by default*);
- la sécurité des données soit assurée;
- les violations de données soient promptement détectées.

Si une violation survient, il faudra la communiquer aux organes internes et, si nécessaire, aux partenaires contractuels, à l'autorité compétente, voire aux personnes concernées.

Un catalogue élargi des droits des personnes concernées

Comme le RGPD, la nLPD introduit le droit à la portabilité des données, soit le droit d'obtenir les données sous un format lisible par machine (par ex. un ordinateur). Si ces requêtes sont fréquentes, il faudra mettre en place des processus afin d'y répondre, cas échéant adapter les processus déjà établis sous le RGPD à la nLPD. Il en va de même du droit d'accès, qui existe déjà et perdurera sous la nLPD.

La menace des nouvelles sanctions

Le non-respect de la nLPD pourra conduire au prononcé de nouvelles sanctions, en particulier des amendes jusqu'à CHF 250 000 imposées à la personne physique fautive (et non (uniquement) à l'entreprise comme c'est le cas avec le RGPD). À cela s'ajoutent en particulier les risques réputationnels en raison de l'importante médiatisation de ces affaires.



Jürg Schneider
Avocat, Dr. en droit, Associé
Walder Wyss SA, Lausanne



Hugh Reeves
Avocat, LL.M., Managing Associate
Walder Wyss SA, Lausanne

Un soutien au travers de la planification et une implémentation proactive

Une mise en œuvre réussie et durable de la nLPD n'est pas obligatoirement compliquée et coûteuse, mais laisse au contraire une certaine marge de manœuvre. Elle nécessite cependant une planification concrète qui tient compte non seulement des particularités de l'entreprise, mais également de son environnement légal et réglementaire et des risques spécifiques auxquels elle est soumise.

L'implémentation de la nLPD doit précéder son entrée en vigueur. Les entreprises doivent donc se montrer proactives à cet égard.

www.walderwyss.com

walderwyss