Kellerhals Carrard

La nouvelle Loi sur la Protection des Données (nLPD)

Julien Rouvinez, Avocat, Associé, Docteur en droit, LL.M.
Vincent Jäggi, Avocat, Associé, Docteur en droit, Master of Advanced Studies (LL.M.) in Business Law (MBL)

ComptaVal
Mercredi, le 22 mars 2023
Hôtel Vatel, Martigny

Kellerhals Carrard

Partie I : Cadre légal

Principes directeurs et nouveautés

1.1. Contexte juridique et social de la révision de la loi en Suisse

Monde
Evolution technologique : outils numériques, Big data, Internet, smart phone, etc.

UE
Révision de la législation européenne en matière de protection des données : entrée en vigueur en mai 2018 du Règlement européen sur la protection des données n° UE 2016/679 (RGPD)

CH
Révision LPD (entrée en vigueur au 1er septembre 2023)

1.1. Loi sur la protection des données : qu'est-ce que c'est?

- «LPD» loi fédérale applicable aux traitements de données par des **personnes privées** ou des **organes fédéraux** (≠ par des organes cantonaux)

► Protection des <u>personnes</u> (sphère privée) – pas des données

1.1. Champ d'application de la LPD et du RGPD pour les entreprises suisses

Application de LPD /nLPD

Application interne : toutes les entreprises traitant des données personnelles en Suisse doivent se conformer aux exigences de la LPD

Portée extra-territoriale : application des la LPD aux états de fait qui se produisent à l'étranger et qui déploient des effets en Suisse

=> le traitement des données a lieu hors de Suisse mais concerne des personnes physiques établies en Suisse:

- le RT doit respecter la législation suisse
- le RT (si hors de Suisse) doit nommer un représentant en Suisse

Application du RGPD à l'étranger et donc en Suisse

Les entreprises qui ne sont pas implantées dans l'UE peuvent relever du champ d'application du RGPD **si elles proposent des biens ou des services à des particuliers ressortissants de l'UE**.

Ex: une boutique en ligne suisse avec un site web disponible en allemand, en français et en anglais. Vous traitez chaque jour plusieurs commandes de particuliers européens et leur envoyez vos produits.

⇒ Application du RGPD, alors même que vous ne possédez aucun établissement au sein de l'UE et que vous n'y exercez aucune activité de traitement des données.

Ex: prestataire de service de stockage de dématérialisé

Ex: service de réseau social ouvert aux utilisateurs de l'UE

Ex: application collectant des données de localisation de citoyens de l'UE à partir de leur smartphone

⇒ Devoir de respecter toutes les obligations du RGPD si vous proposez aussi vos services à des utilisateurs résidant dans l'UE. Peu importe que le service soit gratuit ou payant.

1.1. Obligation de désigner un représentant

Art 14 nLPD

Le responsable du traitement privé qui a son siège ou son domicile à l'étranger désigne **un représentant en Suisse** lorsqu'il traite des données personnelles concernant des personnes en Suisse et que ce traitement remplit les conditions suivantes:

a. le traitement est en rapport avec l'offre de biens ou de services ou le suivi du comportement de personnes en Suisse;

b. il s'agit d'un traitement à grande échelle;

c. il s'agit d'un traitement régulier;

d. le traitement présente un risque élevé pour la personnalité des personnes concernées

Art. 27 RGPD

Obligation pour les responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union

de désigner un représentant

Les responsables du traitement mais aussi les sous-traitants qui ne sont pas établis dans l'Union à y désigner par écrit un représentant, lorsque le RGPD s'applique à leurs activités de traitement.

⇒ Ce représentant doit être établi dans l'un des États membres dans lesquels résident les personnes physiques dont les données à caractère personnel sont traitées dans le contexte de l'offre de biens ou de services qui leur est proposée ou dont le comportement est observé (art. 27 § 3).

1.2. LPD – notions clés

Notions clés	
Données personnelles	Toute information se rapportant à une **personne physique identifiée ou identifiable**
Données sensibles	Données concernant opinions et activités religieuses, philosophiques, politiques ou syndicales, sur la santé, la sphère intime ou l'origine raciale ou ethnique, **données génétiques**, **données biométriques**, données sur les poursuites ou sanctions pénales ou administratives, données sur les mesures d'aide sociale
Traitement	Toute opération relative à des données, notamment la collecte, l'enregistrement, la **conservation**, l'utilisation, la modification, communication, l'archivage, l'effacement ou la destruction

1.2. LPD – notions clés

Notions clés	
Responsable de traitement	La personne privée ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les **finalités** et les **moyens** du traitement de données personnelles
Sous-traitant	La personne qui traite des données personnelles **pour le compte du responsable du traitement**
Personne concernée	La personne physique dont les données personnelles font l'objet d'un traitement

1.2. Principes directeurs de la LPD

Licéité, transparence et bonne foi

Traitements de données ne doivent pas contrevenir à la loi et la personne concernée doit s'attendre à ce qu'un traitement de données ait lieu.

Finalité

Données ne doivent être traitées que pour les finalités préalablement définies et reconnaissables au moment de la collecte.

Proportion-nalité

Données traitées doivent être limitées à ce qui est apte et objectivement nécessaire pour atteindre le but poursuivi.

Exactitude

Le responsable de traitement doit s'assurer que les données traitées sont exactes.

Limitation de la conserva-tion

Les données ne peuvent pas être conservées pour une durée excédant ce qui est nécessaire au regard des finalités.

Sécurité

La sécurité des données doit être assurée par des mesures techniques et organisationnelles.

1.3. Nouveautés de la nLPD

1. Extension de la définition de «données sensibles» aux **données génétiques** et **biométriques** (art. 5 let. c nLPD)

   La définition est différente du RGPD

2. Obligation <u>expresse</u> de détruire ou anonymiser les données qui ne sont plus nécessaires (art. 6 al. 4 nLPD)

1.3. Nouveautés de la nLPD

3. Privacy by design et by default (art. 7 nLPD)

Privacy by design

Dès la conception/planification (*)

– mesures proactives et non réactives, mesures préventives et non correctives

– protection des données de manière automatique avec paramétrage par défaut assurant une protection maximum

– sécurité de bout en bout, pendant toute la période de conservation et mise à jour régulière des mesures de protection

– protection des données compatible avec une fonctionnalité complète

(*) Sylvain Métille, *La notion de protection des données dès la conception*, 9 novembre 2020 in www.swissprivacy.law/26

Privacy by default

- Par défaut, paramètres réglés sur le mode le plus protecteur

1.3. Nouveautés de la nLPD

4. Devoir d'informer lors de la collecte de données (art. 19 nLPD)

Au minimum:

- Identité et coordonnées du responsable de traitement
- Finalité du traitement
- Destinataires ou catégories de destinataires
- Etat(s) vers le(s)quel(s) les données sont communiquées et, le cas échéant, les garanties de protection fournies

→ se munir d'une **politique de confidentialité**

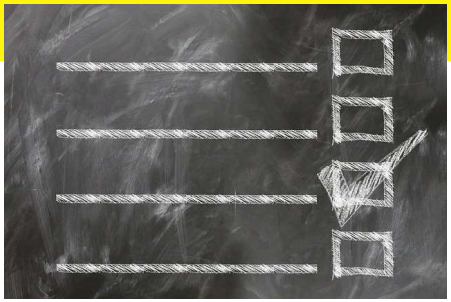
Exceptions prévues (art. 20 nLPD)

1.3. Nouveautés de la nLPD

5. **Conseiller à la protection des données** (Data Protection Officer (DPO)) (art. 10 nLPD)

- Possibilité et non obligation pour les responsables de traitement privés de nommer un DPO
- Interlocuteur des personnes concernées et des autorités
- Mission: former et conseiller, s'assurer de l'application des règles de protection des données
- Connaissances techniques et juridiques
- Employé de la société ou indépendant

1.3. Nouveautés de la nLPD



6. Registre des activités de traitement (art. 12 nLPD)

- Obligatoire pour le responsable de traitement et les sous-traitants (et représentant)
- **Exception pour les PME (inf. à 250 collaborateurs) (art. 24 Opdo) sauf si :**
  - Données sensibles traitées à grandes échelle
  - Traitement constitue un profilage à risque élevé

7. Portabilité des données (art. 28 nLPD)

1.3. Nouveautés de la nLPD

8. **Analyse d'impact (art. 22 nLPD)** : obligatoire en cas de risque élevé

   Auto-évaluation ; Description du traitement prévu et des risques qu'il comporte, ainsi que des mesures appropriées pour contrer ces derniers

9. **Notification des failles de sécurité** (art. 24 nLPD) :

   - Information au PFPDT si risque grave pour la personnalité ou les droits fondamentaux des personnes concernées

   - Information de la personne concernée si nécessaire ou exigé par le PFPDT

1.3. Nouveautés de la nLPD

10. **Représentant en Suisse pour les entreprises étrangères (art. 14-15 nLPD)**

11. **Sanctions pénales** revues à la hausse, néanmoins plus faibles que dans l'UE

    Amende jusqu'à CHF 250'000.- (contre CHF 10'000.- dans aLPD)

    → **visent les personnes physiques responsables**

    → **violation intentionnelles**

Kellerhals Carrard

Partie II. Rôle du conseiller – Plan d’actions et recommandations

Rôle du conseiller → Rappel aux clients

- CA en charge de la haute direction de la société et de fixer les principes de gestion et d'organisation → inclut la mise en conformité à la nLPD, respectivement au RGPD.
- Pas de période transitoire → être prêt au 1er septembre 2023
- Examen attentif des traitements de données; réorganisation; adaptation de la documentation de l'entreprise.
- Saisir l'occasion pour « *construire sa base de données* » (fichier CRM) : digitaliser, nettoyer, consolider.
- Attention aux sanctions pénales → visent les personnes physiques en premier chef; introduction du secret professionnel pour tous

Plan d'actions et Recommandations

- Désigner les responsables à l'interne
- Recenser les données personnelles traitées pour évaluer le risque et déterminer le niveau d'exigence de conformité à appliquer.
  - Ex : traitement de grands volumes de données personnelles : import/export; vente en ligne; entreprises traitant de données sensibles (art. 5nLPD)
- Garantir la sécurité des données selon les principes *privacy by design* et *privacy by default*
- Se conformer au devoir d'information (politique de confidentialité, contrats, etc.)
- Etablir un registre des traitements (si entreprise assujettie à cette obligation)
- Vérifier et adapter les contrats avec les sous-traitants

Plan d’actions et Recommandations (2)

- Vérifier et adapter les flux de données transfrontaliers
- Mettre en place une procédure en cas de violation de sécurité (notification préposé et pers. concernée)
- Mettre en place une procédure en cas de demande d’accès
- Fixer et vérifier la durée de conservation utile, cas échéant
- Détruire les données devenues inutiles
- Formation continue des collaborateurs

Kellerhals Carrard

Merci de votre attention