Monthly
Newsletter
October 2022

Data

Mise en œuvre de la nouvelle loi sur la protection des données: Étape 1 - Préparation

Samuel Klaus, Roland Mathys, Kenzo Thomann

Key Take-aways

1.
La nouvelle loi sur la protection des données entrera en vigueur le 1er septembre 2023, sans période de transition. Les nouvelles exigences doivent être respectées dès le premier jour.

2.
Les mesures de mise en œuvre doivent être préparées à l'avance. L'ordre de priorité des mesures peut être fixé en fonction des risques et des ressources disponibles et la mise en œuvre regroupée en trois étapes.

3.
L'étape 1 comprend la préparation, le bilan de situation et certaines décisions préliminaires. Dans l'étape 2, les mesures externes sont mises en œuvre, dans l'étape 3 les mesures internes.

1 Introduction

Le 31 août 2022, le Conseil fédéral a décidé que la nouvelle loi suisse sur la protection des données (**nLPD**) entrera en vigueur **le 1er septembre 2023**, ainsi que la nouvelle ordonnance y relative (**nOPD**). Il n'y aura pas de période de transition. Néanmoins, une période d'environ un an est ouverte pour la mise en œuvre d'ici à l'entrée en vigueur.

Ce temps doit être utilisé à bon escient et la mise en œuvre des nouvelles exigences doit être lancée rapidement, avec son achèvement planifié pour août 2023 au plus tard. **L'effort requis pour la mise en œuvre** ne doit pas être sous-estimé et dépend de la situation individuelle.

2 Ce qui change - ce qui demeure

Les **principes de base de la loi suisse sur la protection des données** restent les mêmes. Le traitement de données ne requiert ni consentement ni justification spéciale (contrairement au Règlement général sur la protection des données (**RGPD**)), tant que les principes généraux de traitement sont respectés, que la personne concernée ne s'est pas expressément opposée au traitement des données et que les données personnelles sensibles ne sont pas communiquées à des tiers. Les **principes généraux de traitement** (à savoir de licéité, de transparence, de finalité, de proportionnalité, d'exactitude et de sécurité des données) restent également largement les mêmes.

Les changements résultent toutefois du **niveau de détail accru** de la loi, des **exigences formelles** étendues et du **régime de sanctions** nouvellement introduit. En outre, la définition des données personnelles sera restreinte, c'est-à-dire que la nLPD ne concernera que les données des personnes physiques; les personnes morales n'entreront plus dans son champ de protection.

3 Pertinence d'une mise en œuvre rapide

Les exigences de la nLPD doivent être satisfaites dès le 1er septembre 2023. Dès cette date, le nouveau **régime de sanctions** prévoyant des amendes spécifiques sera applicable. Ces amendes (jusqu'à CHF 250'000) ne sont pas comparables à celles prévues par le RGPD (jusqu'à 4 % du chiffre d'affaires mondial ou 20 millions d'euros). La grande différence réside cependant dans le fait que, dans le cadre de la nLPD, les amendes ne visent pas l'entreprise, mais la personne responsable. Il peut s'agir des décideurs officiels (p. ex. la direction, le conseil d'administration) ou des employés ayant un pouvoir de décision propre dans leur domaine d'activité (p. ex. chefs de division ou de département, fonctions centralisées).

4 Mise en œuvre en trois étapes

Il est recommandé d'établir un **ordre de priorité** des mesures de mise en œuvre en fonction des risques et des ressources. **L'effort à prévoir pour la mise en œuvre** dépend de l'attention accordée à la protection des données dans le passé. Si, par exemple, le RGPD a déjà été mis en œuvre (p. ex. en raison des exigences internes au groupe), seuls quelques ajouts aux mesures existantes seront nécessaires. Si seules les exigences minimales de la LPD actuelle ont été mises en œuvre jusqu'à présent (ou même pas), il faut s'attendre à plus de travail.

Nous présentons ci-après un **plan de mise en œuvre** en trois étapes et exposons la première étape de manière détaillée. Les étapes 2 et 3 seront abordées dans deux newsletters ultérieures. Ce plan peut servir de guide mais devra être adapté à la situation concrète dans chaque cas et, cas échéant, complété au vu des exigences spécifiques à l'industrie et au secteur.

5 Calendrier

5.1 Jusqu'à la fin de l'année 2022

Indépendamment de la mise en œuvre des exigences de la nLPD, le Préposé fédéral à la protection des données et à la transparence (**PFPDT**) exige que les **clauses contractuelles types** (*Standard Contractual Clauses* (**SCC**)) **conclues avant le 27 septembre 2021** soient déjà remplacées avant la fin de cette année. Vous trouverez de plus amples informations à ce sujet dans notre newsletter de mai 2022.

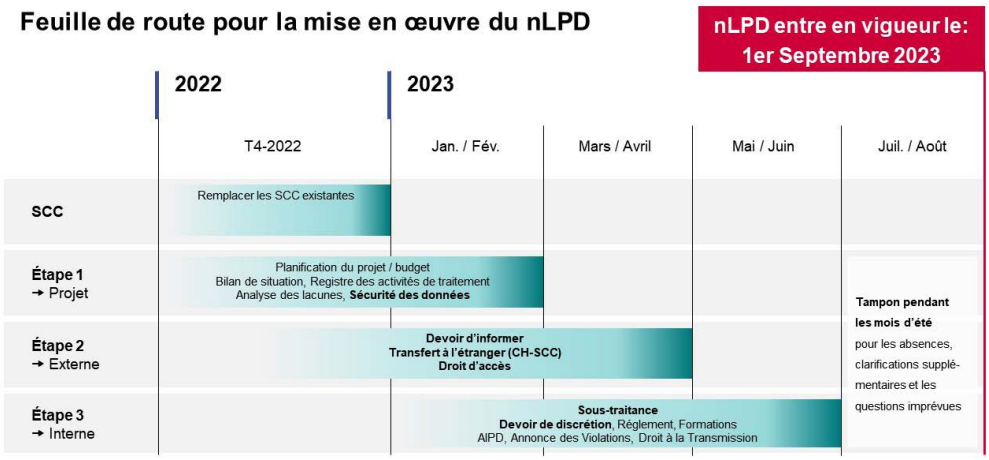
Dans un volet séparé, les transferts de données à l'étranger devront donc être identifiés et traités avec des SCC adaptées au droit suisse **d'ici à fin 2022**. Idéalement, cela pourrait être combiné avec l'étape 1 de la mise en œuvre de la nLPD, en particulier le bilan de situation.

5.2 Feuille de route pour la mise en œuvre de la nLPD

Le calendrier de mise en œuvre dépend dans une large mesure de la manière dont la protection des données a été abordée dans le passé, ainsi que de l'ampleur et de la complexité du traitement de données. En tout état de cause, l'achèvement du projet de mise en œuvre devrait être planifié pour une date avant ou à mi-août 2023. Il convient également de tenir compte des éventuelles absences ou des flux d'informations restreints pendant les mois d'été de juillet/août. Idéalement, cette période devrait être réservée comme tampon. Ainsi, le calendrier suivant peut servir de guide :

- **Du T4-2022 à janvier/février 2023 - Étape 1** : Certaines décisions préliminaires doivent être prises, la coordination du projet (y compris le budget) doit être abordée, et un bilan de situation (y compris des mesures de sécurité des données) peut servir de base à une analyse des lacunes.
- **De novembre/décembre 2022 à mars/avril 2023 - Étape 2** : Focus sur la mise en œuvre de mesures ayant un effet externe (le focus ici dépendra largement du secteur d'activité concerné ainsi que des exigences internes de l'entreprise ou du groupe).
- **De 2023 à mai/juin 2023 - Étape 3** : Focus sur la mise en œuvre de mesures internes (en donnant la priorité aux domaines qui font l'objet de sanctions).

Il est conseillé d'identifier à un stade précoce les domaines dans lesquels un effort plus important est à prévoir en raison de la situation spécifique (p. ex. si des recherches importantes sont à prévoir pour le bilan de situation ou s'il devient évident qu'un grand nombre de contrats doivent être adaptés). Si nécessaire, ces mesures peuvent abordées dès le début.



6 Étape 1 : Préparation

6.1 Évaluation RGPD

À un stade précoce, il convient de se demander si les **exigences du RGPD** doivent être respectées en raison du modèle d'entreprise ou du traitement de données effectué (art. 3 (2) RGPD). Si oui, il faut en tenir compte lors de la mise en œuvre de la nLPD. Dans le cas contraire, la question se pose de savoir si les exigences du RGPD ne doivent pas être mises en œuvre malgré tout (par exemple pour des raisons de réputation ou s'il existe au sein d'un groupe international des processus et documents déjà conformes au RGPD sur lesquels s'appuyer).

S'il existe déjà des processus conformes au RGPD et des documents correspondants, ceux-ci constituent un bon point de départ pour la mise en œuvre de la nLPD. Étant donné qu'il existe encore certaines différences entre la nLPD et le RGPD, certains "**ajouts suisses**" doivent être mis en œuvre en plus des mesures existantes du RGPD. Cela concerne en particulier les domaines des transferts à l'étranger, des déclarations de confidentialité et des demandes d'accès. Vous trouverez plus de détails à ce sujet dans notre newsletter de décembre 2021.

6.2 Coordination du projet

Pour **préparer la mise en œuvre**, il convient de mettre en place très tôt une coordination de projet appropriée, d'identifier et d'impliquer les ressources et personnes de contact nécessaires. Il s'agit en particulier des détenteurs du savoir-faire dans les domaines pertinents (tels que le marketing, l'informatique, les RH), dont la connaissance détaillée des processus internes de l'entreprise et du traitement des données est indispensable pour la mise en œuvre.

6.3 Bilan de situation

Dans le cadre d'un bilan de situation, les informations nécessaires à la mise en œuvre devront être collectées. L'objectif est d'identifier **la collecte actuelle des données**, le **traitement des données** effectué et les éventuels **transferts** de données **à l'étranger**. Comme base pour les étapes suivantes, il convient de documenter de manière facilement accessible qui, dans l'entreprise, collecte, utilise ou traite quelles données personnelles et dans quel but, si cela se fait avec l'aide de prestataires de services externes, si les données personnelles sont transférées à ou accessible depuis l'étranger (et si c'est le cas, quels pays sont concernés), où les données personnelles sont stockées, etc.

Les modèles génériques, les documents existants (par exemple, les registres internes des groupes) et les listes de contrôle concernant les points pertinents peuvent être utiles pour faire le bilan de situation. Si les informations ne sont pas déjà disponibles, elles peuvent être obtenues par des entretiens avec les personnes de contact concernées.

6.4 Registre des activités de traitement

Pour la collecte et la consolidation centralisées des informations, un **registre des activités de traitement** devrait déjà être créé à ce stade (art. 12 nLPD). Il existe une **exception** à l'obligation de tenir un registre des activités de traitement pour les entreprises de moins de 250 employés, à condition qu'aucun traitement à haut risque ne soit effectué (art. 24 nOPD). Cependant, même les entreprises qui bénéficient de cette exemption doivent examiner leurs activités de traitement en détail et mettre en œuvre les autres exigences de la nLPD. Dans la plupart des cas, il est donc conseillé de tenir un registre des activités de traitement, même s'il n'existe aucune obligation légale de le faire.

6.5 Sécurité des données

Comme les évaluations (et les ajustements potentiels) dans le domaine de la **sécurité des données** prennent généralement beaucoup de temps, ce point devrait déjà être abordé à l'étape 1. Par conséquent, dès le bilan de situation, il convient d'examiner et de documenter la portée et l'adéquation des **mesures techniques et organisationnelles** visant à garantir la sécurité des données. La question de savoir si des mesures supplémentaires sont nécessaires ne peut généralement être évaluée qu'en tenant compte des catégories de données identifiées, de leur finalité d'utilisation et du traitement effectué.

La nLPD stipule que l'adéquation des mesures techniques et organisationnelles doit être évaluée sur la base du **besoin de protection** concernant les données en question et du **risque** pour la personnalité ou les droits fondamentaux des personnes concernées, et contient des indications sur la manière de procéder et les critères à respecter (art. 1-5 nOPD).

7 Étapes 2 et 3

Sur la base de la préparation de l'étape 1, **l'étape 2** se concentre sur les **mesures ayant un impact externe** et les conséquences possibles en termes de sanctions. Cela inclut les sujets suivants, que nous aborderons dans la prochaine newsletter :

- Devoir d'information et déclaration de confidentialité
- Droit d'accès
- Transferts à l'étranger

Dans **l'étape 3**, le focus sera mis sur les **mesures, processus et documents internes**, avec une priorisation des domaines sanctionnés par la nLPD. Nous aborderons donc les sujets suivants dans la troisième newsletter :

- Accords de traitement (sous-traitance des données)
- Décisions individuelles automatisées
- Secret professionnel
- Règlement interne de protection des données et formation des employés
- Notification des violations de la sécurité des données
- Analyse d'impact
- Portabilité des données
- Conservation des données et durée de conservation

8 Conclusion et perspectives

La mise en œuvre de la nLPD ne doit pas être prise à la légère. En cas de violation des nouvelles exigences, il existe une menace de sanctions sévères à l'encontre des décideurs. La mise en œuvre en soi n'est pas si complexe, mais elle implique un effort certain et doit être soigneusement planifiée et lancée rapidement.

La mise en œuvre effective peut être structurée en trois étapes, soit **(1) mesures préparatoires**, **(2) mise en œuvre de mesures externes** et **(3) mise en œuvre de mesures internes**. Nous avons décrit la première étape ci-dessus, et nous aborderons les deux autres étapes dans deux prochaines newsletters au cours des prochains mois.

Vincent Carron
Associé Genève
vincent.carron@swlegal.ch

Dr. Catherine Weniger
Conseil Genève
catherine.weniger@swlegal.ch

Roland Mathys
Associé Zurich
roland.mathys@swlegal.ch

Dr. Samuel Klaus
Associé Zurich
samuel.klaus@swlegal.ch

Schellenberg Wittmer SA
Avocats

Zurich
Löwenstrasse 19
Case postale 2201
8021 Zurich / Suisse
T +41 44 215 5252
www.swlegal.ch

Genève
15bis, rue des Alpes
Case postale 2088
1211 Genève 1 / Suisse
T +41 22 707 8000
www.swlegal.ch

Singapour
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapour 049909
T +65 6580 2240
www.swlegal.sg