

N

Monthly
Newsletter
December 2021

**Schellenberg
Wittmer**

Data



Le nouveau droit suisse de la protection des données et les entreprises internationales

Samuel Klaus, Roland Mathys

Key Take-aways

- 1.** La loi suisse révisée sur la protection des données a été alignée sur le RGPD, mais des différences subsistent, qui doivent être prises en compte par les entreprises suisses et internationales faisant des affaires en Suisse.
- 2.** Les processus conformes au RGPD peuvent servir comme base de référence, avec certains "ajouts suisses", afin d'être conformes aux exigences supplémentaires de la loi suisse révisée sur la protection des données.
- 3.** Comme il n'y a pas de période de transition, nous recommandons de commencer la mise en œuvre au début de 2022. Une approche fondée sur les risques peut aider à prioriser les mesures à prendre.

1 Introduction

1.1 Révision de la loi suisse sur la protection des données

La loi suisse sur la protection des données (LPD) a été révisée en 2020, notamment pour l'aligner sur le règlement général sur la protection des données (RGPD) de l'UE. La date d'entrée en vigueur n'est pas encore connue mais probablement pas avant fin 2022, voire début 2023. **Il n'y aura pas de période transitoire.** Dès l'entrée en vigueur de la LPD révisée, ses exigences devront être respectées. Cela aura un impact non seulement sur les entreprises suisses, mais aussi sur toute entreprise internationale ayant une entité ou faisant des affaires en Suisse.

1.2 RGPD comme base de référence

Une entreprise internationale aura en principe **mis en place des processus conformes au RGPD**. En raison d'un établissement en Suisse, ou de l'applicabilité extraterritoriale de la LPD révisée, cette entreprise devra également répondre aux exigences de la LPD révisée. Bien que la révision vise à aligner la LPD sur le RGPD, certaines différences subsistent.

La question qui se pose est donc : Quels sont les **"ajouts suisses"** qui doivent être mis en œuvre en plus des processus RGPD déjà en place ? Dans cet aperçu, nous examinons cette question du point de vue des entreprises internationales.

1.3 Domaines harmonisés

La LPD actuelle diffère de la plupart des autres régimes de protection de données en ce qu'elle concerne les données personnelles relatives à la fois aux personnes physiques et aux personnes morales. La LPD révisée s'appliquera, comme le RGPD, **uniquement aux données personnelles relatives aux personnes physiques**. Cela facilitera les transferts transfrontaliers de données.

L'applicabilité extraterritoriale de la LPD actuelle est très limitée et repose sur le droit international privé suisse. La LPD révisée aura, comme le RGPD, un **champ d'application extraterritorial** et sera donc applicable aux entreprises internationales, sous certaines conditions, même si elles n'ont pas d'établissement en Suisse.

2 Différences pertinentes

2.1 Sanctions

Alors que la LPD actuelle ne contient qu'un régime de sanctions limité avec des amendes allant jusqu'à CHF 10'000, la LPD révisée introduit des **amendes jusqu'à CHF 250'000**. Cela peut sembler peu, comparé aux sanctions prévues par le RGPD, qui peuvent atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial. La grande différence est que, en vertu de la LPD, les amendes **ne visent pas l'entreprise, mais la personne responsable, c'est-à-dire les décideurs et/ou la direction**.

Les sanctions prévues par la LPD révisée s'appliquent en particulier aux obligations liées aux déclarations de protection des données et aux transferts transfrontaliers (cf. sections 2.2 et 2.3 ci-dessous), mais aussi, entre autres, aux

demandes d'accès, aux décisions individuelles automatisées, à l'externalisation et à la sécurité des données. Par contre, ne relèvent pas du champ d'application des sanctions, par exemple, les violations des obligations de notification des violations de données ou de l'obligation de désigner un représentant suisse.

Il faut relever une obligation modifiée concernant le **secret professionnel relatif aux "données personnelles secrètes"**. En vertu de la LPD révisée, quiconque divulgue (intentionnellement, inclus le dol éventuel) des données personnelles secrètes, sera soumis à une amende allant jusqu'à CHF 250'000. Il n'y a pas d'indication à ce jour sur la manière dont cette disposition potentiellement lourde de conséquences sera appliquée par les tribunaux.

Les amendes visent la personne responsable et non l'entreprise.

2.2 Déclarations de protection des données

En vertu du RGPD, la déclaration de protection des données doit contenir une liste étendue de points spécifiques. En vertu de la LPD révisée, cette liste devrait suffire dans la plupart des cas, à l'exception d'une différence importante : Alors qu'en vertu du RGPD, il suffit de mentionner qu'il y a des transferts transfrontaliers (le cas échéant), la LPD révisée exige également **la divulgation des pays cibles**, c'est-à-dire les pays vers lesquels les données sont transférées (ou à partir desquels on y accède).

Pour une entreprise internationale, en lien avec les entités du groupe ou les prestataires de services tiers, cela peut s'avérer être un véritable défi. L'énumération de régions géographiques plutôt que de pays spécifiques peut être une solution, s'il reste possible pour la personne concernée d'identifier les pays spécifiques (p.ex., il est clair quels pays appartiennent à l'UE, mais pas lesquels seraient concernés par une référence à l'Asie).

Une déclaration de protection des données existante au titre du RGPD peut donc constituer une base solide pour une utilisation dans le cadre de la LPD révisée, mais devra être modifiée au moins en ce qui concerne les transferts transfrontaliers, et éventuellement aussi en ce qui concerne la formulation visant à limiter l'applicabilité potentielle de l'obligation de secret professionnel mentionnée à la section 2.1. Comme les violations des obligations d'information **sont passibles de sanctions** en vertu de la LPD révisée, il convient d'être prudent à cet égard.

2.3 Transferts transfrontaliers

L'approche des transferts transfrontaliers est identique dans le cadre du RGPD et de la LPD révisée, ces transferts ne né-

cessitant pas de mesures supplémentaires s'ils sont effectués vers un "pays sûr", mais exigeant des garanties supplémentaires s'ils sont effectués vers des pays ne disposant pas d'un niveau adéquat de protection des données. Dans le cadre du RGPD, ces garanties consistent le plus souvent en les nouvelles **clauses contractuelles types de l'UE (UE-SCC)**.

L'autorité suisse de protection des données, le Préposé fédéral à la protection des données et à la transparence (PFPDT), a récemment accepté les UE-SCC comme des garanties appropriées en vertu de la législation suisse sur la protection des données, **sous réserve de certaines modifications requises par la législation suisse (CH-SCC)**. L'ampleur de ces modifications dépend de la nature des données et du transfert en question. Souvent, une entreprise internationale aspirera à aligner le CH-SCC sur le UE-SCC. Les directives publiées par le PFPDT le permettent, certains "ajouts suisses" obligatoires restant cependant nécessaires.

Le UE-SCC peut donc être un bon point de départ pour les transferts transfrontaliers soumis à la LPD, mais devra être **modifié (p.ex. avec un "Swiss Rider")** pour remplir les exigences du PFPDT. Les transferts transfrontaliers étant un domaine **soumis à des sanctions** en vertu de la LPD révisée, cette matière doit être abordée avec diligence.

2.4 Notification des violations de données

Alors que le RGPD autorise la notification des violations dans un délai de 72 heures, la LPD révisée exige une notification aussi rapide que possible. En outre, en vertu de la LPD révisée, les seuils de risque déclenchant une obligation de notification à l'autorité de protection des données et/ou aux personnes concernées sont définis de manière légèrement différente de ceux du RGPD. Il pourrait donc être nécessaire de **définir des processus et des directives internes distincts pour les violations ayant un lien avec la Suisse**. Contrairement à ce qui est prévu par le RGPD, dans le cadre de la LPD révisée, la violation des obligations de notification des violations n'est pas soumise à des sanctions.

2.5 Représentant suisse

En vertu du RGPD, une entité domiciliée en dehors de l'UE, p.ex. une société suisse, doit, sauf quelques exceptions, désigner un représentant dans l'UE si cette entité est soumise à l'applicabilité extraterritoriale du RGPD. La LPD révisée reprend cette exigence, mais de manière moins étendue.

Par conséquent, les entreprises internationales qui n'ont pas d'entité suisse, mais qui font des affaires en Suisse, **ne devront désigner un représentant suisse qu'en cas de traitement étendu à haut risque**. Ce pourrait être le cas, p.ex., de services numériques liés à la santé, traitant régulièrement une quantité significative de données relatives à la santé. En cas de traitement régulier de données sensibles concernant des résidents suisses, il convient donc de vérifier si un représentant suisse doit être désigné. Les violations de cette obligation ne sont pas soumises à des sanctions.

2.6 Autres sujets pertinents

La LPD révisée contient un devoir d'information plus spécifique concernant les **décisions individuelles automatisées, passible de sanctions**. Une entreprise internationale qui utilise des décisions individuelles automatisées concernant

des résidents suisses devrait donc vérifier les processus sous-jacents et les directives internes.

En outre, la LPD révisée ne prévoit pas de liste spécifique d'informations à fournir en cas de **demande d'accès des personnes concernées**, mais contient plutôt une clause générale étendue - les violations **étant passibles de sanctions**. Une entreprise internationale devrait donc vérifier les procédures et documents correspondants, fondés sur le RGPD, avant de les mettre en œuvre dans le cadre de la LPD révisée.

Concernant le **registre de traitement**, requis à la fois par le RGPD et la LPD révisée, le registre basé sur le RGPD peut être utilisé pour la Suisse, avec quelques modifications le cas échéant (p.ex., concernant les pays cibles en cas de transfert transfrontalier; cf. section 2.3). Les entreprises de moins de 250 employés seront exemptées de l'obligation de tenir un registre, si leur traitement de données ne comporte qu'un faible risque.

3 Comment assurer la conformité

Les processus et la documentation existants relatifs au RGPD constituent un bon point de départ. L'étape supplémentaire pour assurer la conformité avec la LPD révisée n'est pas insurmontable mais néanmoins nécessaire. Elle doit être traitée avec rigueur.

La LPD révisée **ne prévoyant pas de période de transition**, il est recommandé de se préparer au début de 2022 afin d'être prêt lorsque la LPD révisée entrera en vigueur - avec des sanctions visant la personne responsable et/ou la direction.

Une approche basée sur les risques peut aider à **définir les sujets centraux** et à allouer les ressources le plus efficacement. D'une manière générale, et sous réserve de l'alignement avec (a) le régime spécifique de protection des données déjà mis en œuvre par une entreprise internationale, (b) la nature des données personnelles et du traitement concerné, et (c) la relation spécifique avec la Suisse et la LPD révisée, on peut aborder la mise en œuvre à l'aide d'une liste de mesures classées par ordre de priorité:

High Risk	Transferts transfrontaliers : Évaluer les transferts transfrontaliers de données concernant les résidents suisses et mettre en place des mesures de protection conformes à la LPD (par exemple, CH-SCC).
Medium Risk	Déclarations de protection des données : Passer en revue les déclarations de protection des données existantes fondées sur le RGPD et les modifier en fonction des exigences supplémentaires de la LPD révisée, dans la mesure nécessaire.
	Demandes d'accès / Décisions individuelles automatisées : Vérifier les processus existants en fonction des exigences de la LPD révisée.

Low Risk	<p>Notification des violations de données : Fournir un processus distinct et des directives internes alignés sur les exigences de la LPD révisée.</p>
	<p>Représentant suisse : Évaluer si, sur la base du traitement des données concernant les résidents suisses, il est nécessaire de désigner un représentant suisse.</p>
	<p>Registre de traitement : Évaluer si un registre de traitement doit être tenu en vertu de la LPD révisée et, le cas échéant, modifier le registre existant basé sur le RGPD avec les informations supplémentaires requises en vertu de la LPD révisée.</p>

4 Conclusion

L'entrée en vigueur de la LPD révisée rapprochera le droit suisse de la protection des données du RGPD. Certaines différences subsisteront et devront être respectées par les entreprises internationales ayant des entités ou des activités en Suisse, en raison de l'applicabilité extraterritoriale de la LPD révisée.

Les principaux domaines comportant des "ajouts suisses" concernent les transferts transfrontaliers, les déclarations de protection des données et les demandes d'accès. La non-conformité dans ces domaines peut entraîner des sanctions (amendes jusqu'à CHF 250'000). Comme la LPD révisée devrait entrer en vigueur à la fin de 2022 ou au début de 2023 sans période de transition, les mesures nécessaires pour assurer la conformité doivent être prises dès maintenant.



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

Le contenu de cette Newsletter ne peut pas être assimilé à un avis ou conseil juridique ou fiscal. Si vous souhaitez obtenir un avis sur votre situation particulière, votre personne de contact habituelle auprès de Schellenberg Wittmer SA ou l'une des personnes mentionnées ci-dessus répondra volontiers à vos questions.

Schellenberg Wittmer SA est votre cabinet d'avocats d'affaires de référence en Suisse avec plus de 150 juristes à Zurich et Genève ainsi qu'un bureau à Singapour. Nous répondons à tous vos besoins juridiques – transactions, conseil, contentieux.



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