AVOCATS

SCHELLENBERG WITTMER

MARS 2017

Newsletter

Auteurs:
Roland Mathys
Samuel Klaus



PROTECTION DES DONNÉES

Points pertinents de la révision de la loi sur la protection des données

La révision de la loi suisse sur la protection des données s'inspire fortement du règlement général de l'UE en la matière, ce qui révèle le souci du législateur de s'assurer que le régime suisse continue à être considéré comme suffisant par ses voisins européens. L'avant-projet comporte également des nouveautés pour les responsables du traitement des données, les sous-traitants et les personnes concernées. Cette newsletter analyse les changements prévus sous l'angle de ces trois cercles d'intéressés.

1 ÉTAT DE LA RÉVISION

Alors que les travaux en vue de la révision de la loi suisse sur la protection des données (**LPD**) courent déjà depuis fin 2010, l'avant-projet de loi a été publié fin 2016 (**AP-LPD**). En raison du grand nombre de commentaires auquel il faut s'attendre dans le cadre de la consultation ouverte jusqu'au 4 avril 2017, les résultats consolidés sous forme d'un projet avec son message à l'attention de l'assemblée fédérale ne devraient être disponibles qu'en fin d'année.

L'AP-LPD prend notamment en compte les exigences du règlement général sur la protection des données de l'UE (**UE-RGPD**) et la convention révisée du Conseil de l'Europe STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ceci afin d'attester d'un niveau de protection suffisant conféré par la législation suisse vis-à-vis de l'UE. De plus, l'AP-LPD contient plusieurs durcissements comparé à la LPD en vigueur. Bien que l'avant-projet ne soit probablement pas repris intégralement dans le projet de révision final, il convient néanmoins de traiter de ces évolutions par égard aux entreprises dont le modèle économique sera fortement affecté par les nouveautés proposées.

Sont ainsi présentés ci-après les aspects pertinents de la révision de la LPD du point de vue du responsable du traitement (*Controller*), du sous-traitant (*Processor*) et de la personne concernée (*Data Subject*).

2 RESPONSABLE DU TRAITEMENT

La dénomination actuelle du maître du fichier est remplacée par le responsable du traitement, de laquelle découlent de nouvelles obligations d'information et de prise de mesures. Leur respect est assuré par des normes pénales plus sévères que celles du droit actuel, mais qui n'atteignent toutefois pas le degré de sévérité des amendes prévues par l'UE-RGPD.

2.1 NOUVELLES OBLIGATIONS D'INFORMATION

Lors du relèvement et de la collecte de données personnelles, le responsable du traitement a un devoir d'information qui va **au-delà des obligations d'information actuelles**. L'une des principales nouveautés est l'obligation de communiquer l'identité et les coordonnées du sous-traitant si le traitement lui est confié. Une autre nouveauté s'agit de l'obligation d'information qui pèse sur le responsable dans l'hypothèse d'une violation de la protection des données à cause d'un traitement non autorisé ou de toute perte de données (*Data Breaches*). La violation ou perte doit en premier lieu être notifiée au préposé fédéral à la protection des données et à la transparence (**Préposé**) puis à la personne concernée lorsque cela est nécessaire à sa protection (p.ex. lors de perte de données de carte de crédit, d'identifiants).

2.2 NOUVELLES OBLIGATIONS DE PRISE DE MESURES

Lorsque le traitement envisagé est susceptible d'entraîner un risque accru pour la personne concernée, le responsable du traitement doit procéder au préalable à une **analyse d'impact** (*Privacy Impact Assessment*). Aussi bien son résultat que la totalité du traitement des données sont à documenter. Cette **obligation de documentation** remplace la présente obligation de déclarer certains fichiers.

De plus, le résultat de l'analyse d'impact ainsi que les mesures de réduction des risques prévues sont à annoncer au Préposé, qui détient la possibilité d'émettre des objections à leur encontre dans un délai de trois mois.

> "L'avant-projet prévoit la *Privacy by Design* et la *Privacy by Default* et des dispositions pénales pour en assurer le respect."

Comme à l'heure actuelle, le responsable du traitement doit garantir la **sécurité des données**; toutefois, contrairement à ce qui prévaut aujourd'hui, celui-ci peut se voir infligé une amende s'il omet de prendre les mesures nécessaire. Est également punit d'une amende, l'omission, par le responsable du traitement, de prendre les mesures prescrites en lien avec la ***Privacy by Design*** (la protection des données dès la conception) et la ***Privacy by Default*** (réglages par défauts en faveur de la protection des données). La *Privacy by Design* comprend les mesures préventives techniques et organisationnelles (p.ex. l'anonymisation); la *Privacy by Default* requière que les réglages prédéfinis traitent uniquement les données personnelles visées et seulement autant que nécessaire.

L'introduction des **recommandations de bonnes pratiques** (**Best Practices**) pourra toutefois représenter un soulagement pour les responsables du traitement: en effet, si le responsable du traitement s'y conforme, il se comporte, selon la définition de la loi, conformément aux dispositions de protection des données personnelles que l'AP-LPD prévoit. Les Best Practices sont édictées par le Préposé ou par des opérateurs privés, puis approuvées par le Préposé le cas échéant.

2.3 DISPOSITIONS PÉNALES SÉVÈRES

Dans l'AP-LPD, le champ d'application des dispositions pénales est sensiblement élargi: est punissable aussi bien la violation du devoir d'informer, du droit d'accès, que celui de documentation. Qui ne se conforme pas à une décision du Préposé, communique des données à l'étranger sans s'assurer d'un niveau de protection adapté, confie le traitement à un sous-traitant de manière illicite ou n'assure pas une sécurisation adéquate des données sera désormais punissable. Une telle sanction vient également à s'appliquer en cas d'omission d'entreprendre une analyse d'impact ainsi que de violation du devoir de *Privacy by Design* ou de *Privacy by Default*.

Des **amendes allant jusqu'à CHF 500'000 pour les infractions commises intentionnellement** et jusqu'à **CHF 250'000 en cas de négligence** sont prévues. Ces montants sont certes élevés en comparaison des actuels, mais demeurent assez bas relativement aux amendes de l'UE-RGPD. Contrairement à ce qui est le cas en droit de la concurrence, il s'agit ici non pas de sanctions administratives à l'encontre de l'entreprise, mais plutôt de sanctions pénales contre l'individu responsable (p.ex. l'employé d'une entreprise). Si cette conception apparaît effectivement justifiée, son efficacité semble douteuse.

3 SOUS-TRAITANT

Contrairement à la réglementation actuelle, celui qui traite des données personnelles pour le compte du responsable du traitement est nouvellement défini dans l'AP-LPD comme le **sous-traitant**. Tandis que le droit actuel ne prévoyait que quelques provisions sporadiques à son sujet, l'AP-LPD le soumet à divers obligations et sanctions correspondantes.

3.1 NOUVELLES OBLIGATIONS IMPORTANTES

S'agissant de plusieurs nouvelles obligations prévues, le sous-traitant est obligé de les respecter directement, soit cumulativement soit alternativement au responsable du traitement. Ainsi, il doit p.ex. assurer la sécurité des données, documenter leur traitement et mettre en œuvre les principes de Privacy by Design et de Privacy by Default de la même manière que le responsable du traitement. En ce qui concerne l'analyse d'impact, le sous-traitant et le responsable du traitement sont obligés alternativement l'un à l'autre, mais sont tous deux soumis aux même régime de sanctions.

Le sous-traitant a également le devoir d'informer le responsable du traitement en cas d'une violation de la protection des données (traitement non autorisé, ***Data Breaches***) pour permettre à ce dernier de prendre connaissance de son obligation d'information envers le Préposé et, le cas échéant, les personnes concernées.

3.2 SUBPROCESSING UNIQUEMENT AVEC ACCORD

Si le sous-traitant souhaite lui aussi confier le traitement des données (ou une partie) à un autre sous-traitant (*Sub-Processor*), **l'accord écrit préalable du responsable du traitement** est requis. Ceci peut être effectué par le tru-

chement d'une déclaration générale d'accord. Le cas échéant, le sous-traitant doit toutefois informer le responsable du traitement de tout changement subséquent pour que ce dernier ait la possibilité de s'y opposer. Ainsi, le responsable du traitement est garanti de pouvoir remplir ses obligations d'information envers la personne concernée.

3.3 PASSIBLE DE SANCTIONS PÉNALES

Le sous-traitant est également nouvellement soumis, au même titre que le responsable du traitement, à des dispositions pénales plus sévères avec des amendes **jusqu'à CHF 500'000 pour des violations intentionnelles et jusqu'à CHF 250'000** en cas de négligence.

> "Le sous-traitant est soumis à de nouvelles obligations et sanctions correspondantes."

4 LA PERSONNE CONCERNÉE

L'AP-LPD prévoit également des nouveautés pour les **personnes concernées** dont les données sont traitées. D'une part, la protection ne devrait s'appliquer qu'aux personnes physiques et, d'autre part, la définition des données personnelles sensibles de même que le droit d'accès devraient être étendus.

4.1 UNIQUEMENT LES PERSONNES PHYSIQUES

Alors que le droit en vigueur protège aussi bien les personnes physiques que morales, seules les données de personnes physiques devraient tomber dans le champ d'application de la loi nouvelle. Le législateur renonce ainsi à la protection des données des personnes morales, en contrepartie de quoi leurs communications s'en retrouveraient simplifiées à l'étranger, où une telle protection n'existe généralement pas. En renonçant à l'exception suisse en la matière, la transmission de données envers des états tiers serait dès lors facilitée, raison pour laquelle une telle nouveauté serait la bienvenue.

4.2 DONNÉES PERSONELLES SENSIBLES

La définition de données personnelles sensibles est étendue aux données génétiques (comme p.ex. un profil ADN) et biométriques, qui identifient un individu de façon unique: relèvent p.ex. des données biométriques les images du visage, les scans de l'iris et les empreintes digitales (qu'on utilise en particulier pour déverrouiller un Smartphone).

4.3 DROIT D'INFORMATION ET D'ACCÈS

La révision de la LPD doit particulièrement améliorer la transparence du traitement des données. À cette fin, d'une part, les obligations d'information du côté du responsable du traitement sont renforcées (cf. plus haut section 2.1); d'autre part, le contenu du droit d'accès des personnes concernées est élargi et il est décrit plus clairement quelles informations doivent être fournies par le responsable du traitement.

De plus, l'obligation de renseigner de manière correcte est **assortie de sanction**: qui fournit intentionnellement des renseignements inexacts ou incomplets est puni d'une **amende jusqu'à CHF 500'000**.

Par ailleurs, la manière de traiter les **données de personnes** décédées est désormais définie et prévoit en particulier que, les proches peuvent consulter les données du défunt et en exiger la destruction.

5 REMARQUES FINALES

L'AP-LPD contient des nouveautés pour tous les cercles d'intéressés. Les **responsables du traitement** sont touchés de manière prépondérante concernant le traitement des données car ils se voient imposé une série de nouvelles obligations comportant, en cas de violation, des sanctions considérables.

De même, les **sous-traitants**, qui n'étaient jusqu'à présent que très peu visés directement par la loi, sont nouvellement rendus davantage responsables. L'AP-LPD les oblige en bien des situations cumulativement ou alternativement au responsable du traitement et les expose aux mêmes sanctions pénales.

L'avant-projet comporte également des changements pertinents pour les **personnes concernées**. Tandis que les personnes morales sont entièrement exclues du champ de protection, les droits d'information et d'accès des personnes physiques devraient être renforcés.

Il faut garder à l'esprit que les propositions contenues dans l'AP-LPD ne seront peut-être pas toutes retenues et mises en œuvre: dans une première phase, les résultats de la procédure de consultation seront intégrés dans le projet soumis au parlement; dans une deuxième phase, il faudra s'attendre à d'intensives délibérations dans les chambres et à l'intervention d'une population maintenant très intéressée et sensible aux questions de protection des données.

Bien que l'UE-RGPD sera d'application directe à partir du 25 Mai 2018 et touchera également les entreprises suisses de manière directe ou indirecte, **il ne faut pas pour autant s'attendre à ce que le nouveau droit de la protection des données révisé suisse soit déjà entré en vigueur à cette date**. Toutefois, il est recommandé aux entreprises suisses de suivre les développements avec assiduité et d'adapter au plus vite leurs protocoles internes de protection des données aux évolutions se profilant à l'horizon. En se tenant à des efforts d'implémentation préventive, l'adaptation simultanée de la structure de compliance aux exigences du UE-RGPD d'une part et à celles de la LPD suisse révisée de l'autre pourrait éventuellement être évitée.

> "Les entreprises suisses devraient suivre la révision de la LPD attentivement pour éviter de devoir adapter leur structure de compliance au UE-RGPD d'une part, puis à la LPD révisée d'autre."

Contacts

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'un des avocats suivants répondra volontiers à vos questions:

A Genève:



Vincent Carron

Associé
vincent.carron@swlegal.ch



Catherine Weniger

Conseil
catherine.weniger@swlegal.ch

A Zurich:



Roland Mathys

Associé
roland.mathys@swlegal.ch



Samuel Klaus

Avocat
samuel.klaus@swlegal.ch

SCHELLENBERG WITTMER SA / Avocats

ZURICH / Löwenstrasse 19 / Case postale 2201 / 8021 Zurich / Suisse / T +41 44 215 5252
GENÈVE / 15bis, rue des Alpes / Case postale 2088 / 1211 Genève 1 / Suisse / T +41 22 707 8000
SINGAPOUR / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapour 049909 / www.swlegal.sg

www.swlegal.ch

Cette Newsletter est disponible en français, anglais et allemand sur notre site internet www.swlegal.ch.