Pestalozzi Update Février 2017

Le projet de révision de la loi sur la protection des données – nouvelles obligations et conséquences pour les entreprises

L'avant-projet de révision totale de la loi suisse sur la protection des données (LPD) a été mis en consultation en décembre 2016. La révision a notamment pour but de renforcer la protection des données et de l'adapter à la modification des conditions technologiques et sociales. Dans cette optique, l'équivalence du droit suisse avec le doit européen en matière de protection des données revêt une importance centrale afin que le flux de données transfrontières reste facilité.

La révision a en particulier pour but d'augmenter la transparence lors du traitement des données personnelles, ainsi que de permettre un meilleur contrôle par les personnes concernées sur leurs propres données. Afin de satisfaire aux exigences de la loi révisée, les entreprises auront à l'avenir l'obligation, à chaque fois qu'elles traiteront des données, d'anticiper les violations possibles à la protection des données. En compensation, elles n'auront plus à déclarer les collectes de données.

1. Eurocompatibilité

Dans le cadre de l'accord d'association à Schengen, la Suisse s'est engagée à reprendre la nouvelle **directive UE 2016/680** sur la protection des données. Le Conseil de l'Europe est en outre en train de réviser la Convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel que la Suisse souhaite ratifier.

- **Le projet de révision entraînera plus de responsabilités et plus d'obligations pour les entreprises.**
- **Les entreprises devront traiter les données des personnes physiques de manière plus transparente et satisfaire à leur obligation d'information afin que les personnes physiques puissent faire valoir leurs droits.**
- **En cas de violation de la protection des données, les entreprises seront frappées de sanctions sévères.**

Le besoin d'adaptation au droit européen et l'équivalence entre le droit suisse et le droit européen sont d'une importance centrale pour l'économie suisse,

en particulier pour la garantie et l'amélioration de la **compétitivité** de la Suisse: c'est en effet le seul moyen pour que l'UE reconnaisse la Suisse comme un Etat tiers avec un niveau de protection des données adéquat et pour que la transmission simplifiée transfrontière des données reste possible à l'avenir. Un niveau de protection élevé reconnu à la Suisse au niveau international favorise en outre le développement de nouvelles branches économiques dans le domaine de la société numérique.

2. Modifications pertinentes pour les entreprises

Toutes celles et ceux qui traitent des données sont soumis à la loi sur la protection des données. **Toutes les entreprises actives en Suisse** sont par conséquent concernées par les modifications prévues dans l'avant-projet. Les entreprises qui déterminent les finalités, les moyens et l'étendue du traitement des données personnelles seront considérées dans le cadre de la loi révisée sur la protection des données comme les **responsables** du traitement des données (art. 3 lit. h de l'avant-projet de la révision de la LPD, correspondant à l'art. 3 (8) de la Directive UE 2016/680).

Selon l'avant-projet, les données des personnes morales ne tomberont à l'avenir plus dans le champ de protection de la loi (art. 1 de l'avant-projet de la LPD). Cela facilitera la communication des données des personnes morales à des Etats étrangers (qui bien souvent en effet, ne prévoient aucune protection des données des personnes morales dans leur législation). Les **données des personnes morales ne seront ainsi plus protégées par la LPD**. Une protection globale identique sera toutefois toujours offerte par d'autres lois (art. 28 ss CC, LCD, LDA etc.). Les profils de la personnalité ne seront plus protégés non plus, ce qui était jusque-là considéré comme une particularité du droit suisse; seul le **profilage**, c'est-à-dire toutes les formes de traitement automatisé des données à caractère personnel, sera soumis à la protection des données (art. 3 lit. f de l'avant-projet de la LPD) et nécessitera le consentement exprès de la personne concernée (art. 4, al. 6, art. 23 al. 2 lit. d de l'avant-projet de la LPD).

La **transparence** de mise pour les entreprises lors du traitement des données doit être améliorée et renforcée. Le **devoir d'information** des personnes concernées en cas de collecte de données (et pas seulement pour les données sensibles) sera ainsi étendu à tous les traitements de données (art. 13 de l'avant-projet de la LPD) et englobera toutes les informations nécessaires pour que les personnes concernées puissent faire valoir leurs droits. Les entreprises pourront toutefois satisfaire à cette obligation d'information de façon globale plutôt qu'individuelle (p. ex. via des Conditions générales ou d'une autre façon facilement accessible et compréhensible). Les personnes concernées devront en outre être informées des décisions qui reposent exclusivement sur un traitement automatisé des données (art. 15 de l'avant-projet de la LPD). Elles devront dans ce cas avoir l'occasion de présenter leur point de vue. Les entreprises devront publier d'autres informations lorsque les personnes concernées feront valoir leur droit d'accès élargi au sens de l'art. 20 de l'avant-projet de la LPD, ou si des données à caractère personnel devaient être transmises à des tiers (art. 19 lit. b de l'avant-projet LPD).

La révision de la LPD entraînera surtout des **obligations de diligence et d'annonce** pour les entreprises: celles-ci seront ainsi obligées d'effectuer un contrôle à chaque fois qu'elles traiteront des données et, en cas de risque accru pour les droits des personnes concernées, seront également tenues d'annoncer au Préposé fédéral à la protection des données et à la transparence (PFPDT) les mesures de protection provisoires prévues. Les violations de la protection des données au sens de l'art. 17 de l'avant-projet de la LPD devront en outre être notifiées sur-le-champ au PFPDT et à la personne concernée lorsque cela est nécessaire à sa protection par le responsable du traitement des données. Lors du contrôle du traitement des données, l'entreprise pourra se référer aux recommandations de bonnes pratiques publiées par le PFPDT (art. 8-9 de l'avant-projet de la LPD).

Il s'ensuit que **l'autorégulation** et la **responsabilité propre** des entreprises joueront un rôle central. Les prescriptions sur la protection des données devront être examinées par les entreprises **dès la conception et par défaut** déjà lors de la planification de nouveaux traitements de données afin de réduire ou prévenir les risques d'atteintes à la personnalité (art. 18 de l'avant-projet de la LPD). De manière standard, il faudra choisir la solution la plus respectueuse de la protection des données, avec la conséquence que les entreprises seront autorisées à collecter et traiter moins de données qu'à l'heure actuelle. Les entreprises devront en outre documenter tous leurs processus de traitement des données (art. 19 de l'avant-projet de la LPD).

En ce qui concerne la **transmission des données** à l'étranger, les règles existantes seront en principe toujours applicables. Les données personnelles ne devront pas être communiquées à l'étranger si cela devait comporter le risque de porter gravement atteinte à la personnalité des personnes concernées, ce qui sera notamment le cas si la législation de l'Etat concerné devait ne pas garantir de protection adéquate (art. 5 de l'avant-projet de la LPD). Les contrats de transmission des données (basés sur le contrat-type du Conseil de l'Europe), les contrats internationaux (comme le nouveau Privacy Shield pour la transmission entre les USA et la Suisse) ainsi que les dispositions contraignantes internes des entreprises relatives à la protection des

données approuvées au préalable par le PFPDT ou par une autorité étrangère ad hoc seront considérées comme garantissant une protection des données adéquate (art. 5 al. 3 de l'avant-projet de la LPD). La communication de données à l'étranger sera également autorisée lorsqu'elle est indispensable à la constatation, à l'exercice ou à la défense d'un droit devant une autorité administrative, p. ex. les autorités fiscales (art. 6 al. 1 lit. c de l'avant-projet de la LPD).

Le PFPDT veillera à la mise en œuvre de l'autorégulation. Son rôle se verra ainsi renforcé et ses compétences étendues (art. 41 ss de l'avant-projet de la LPD). Il pourra édicter des recommandations de bonnes pratiques, qui pourront être utilisées comme base par les sociétés pour créer leurs propres recommandations (art. 8 de l'avant-projet de la LPD. De même, le PFPFT pourra, d'office ou sur dénonciation, ouvrir une enquête contre des entreprises pour vérifier la licéité du traitement des données, puis rendre une décision contraignante à l'encontre de ces entreprises. Cela permettra notamment un meilleur contrôle de l'application et le respect des dispositions sur la protection des données.

3. Renforcement des dispositions pénales/des sanctions

Pour que les nouvelles obligations inscrites dans la loi sur la protection des données soient respectées de manière stricte par les responsables du traitement des données, la liste des comportements punissables sera adaptée à ces nouvelles obligations et les dispositions sur les sanctions seront renforcées. L'amende maximum sera relevée de CHF 10'000.- à CHF 500'000.- (art. 50 et ss de l'avant-projet de la LPD).

Une nouvelle obligation incombera au PFPDT, à savoir la notification de tout fait délictueux au sens des art. 50 ss de l'avant-projet de la LPD aux autorités pénales. Les personnes morales pourront ainsi être poursuivies directement devant les autorités pénales sur la base de l'art. 53 de l'avant-projet de la LPD.

4. Recommandations

La révision de la loi renforcera clairement la protection de la personnalité des personnes physiques lors du traitement des données. Si le projet n'en est encore qu'au stade de la consultation, il n'y a cependant pas lieu de s'attendre à une résistance marquée. Il est en effet très important que la solution suisse continue à être compatible avec la nouvelle Directive UE 2016/680.

De nouvelles tâches et de nouvelles obligations incomberont aux entreprises. Les entreprises doivent consacrer aujourd'hui déjà une attention suffisante à la protection des données et aux questions de régulation, ainsi que contrôler la gestion interne relative aux données personnelles et appliquer les standards nécessaires. Le besoin de mise en conformité ne devra pas être sous-estimé et les entreprises doivent se préparer à mettre en œuvre la loi révisée sur la protection des données. En particulier s''il n'en existe pas encore, elles devraient songer à créer une infrastructure et des règles internes contraignantes de protection des données.

Questions sur le contrôle pour les entreprises	
1	Les données personnelles sont-elles traitées en toute bonne foi, sur la base du but indiqué et de manière proportionnelle?
2	Satisfaisons-nous correctement à notre obligation d'information dans le cadre du traitement des données personnelles?
3	Appliquons-nous au traitement des données la protection des données dès la conception et par défaut?
4	La transmission des données à l'étranger est-elle effectuée dans le respect d'une protection adéquate?
5	Possédons-nous une infrastructure de conformité qui nous permet de contrôler le traitement des données?

Nous vous conseillons volontiers personnellement sur les démarches nécessaires pour que votre entreprise puisse respecter la loi révisée sur la protection des données.

Pour de plus amples informations, allez sur notre site Internet ou contactez:

Me Lorenza Ferrari Hofer
Associée
Responsable du groupe IP&TMT
lorenza.ferrari@pestalozzilaw.com
+41 217 92 57

Me Michèle Burnier
Associée

michele.burnier@pestalozzilaw.com
+41 22 999 96 31

Pestalozzi Avocats SA

Zurich - Löwenstrasse 1 | 8001 Zurich | Suisse | T +41 44 217 91 11
Genève - Cours de Rive 13 | 1204 Genève | Suisse | T +41 22 999 96 00

www.pestalozzilaw.com