Novembre 2020

Newsletter n° 146

La révision de la Loi fédérale sur la protection des données – Recommandations de mise en œuvre

La révision de la Loi sur la protection des données devrait probablement entrer en vigueur en début ou milieu d'année 2022. Elle ne contient que peu de périodes transitoires pertinentes en pratique – les obligations telles que le devoir d'information, l'obligation d'effectuer une analyse d'impact relative à la protection des données ou de signaler les violations de la sécurité des données s'appliqueront en grande partie dès l'entrée en vigueur. Le respect en temps voulu de ces obligations nécessite une préparation. Les objectifs et la portée des projets de mise en œuvre varient considérablement, en fonction, par exemple, de la taille et de la complexité de l'entreprise, du modèle d'affaires, des attentes vis-à-vis du secteur concerné et du fait que des exigences du Règlement général sur la protection des données (RGPD) auraient déjà été mises en œuvre. Une approche pragmatique et ciblée est essentielle.

walderwyss avocats

De Jürg Schneider
Dr. iur., avocat
Associé
Téléphone direct: +41 58 658 55 71
juerg.schneider@walderwyss.com

et David Vasella
Dr. iur., avocat
Associé
Téléphone direct: +41 58 658 52 87
david.vasella@walderwyss.com

et Lena Götzinger
Avocate (Chambre des avocats de Frankfurt am Main)
Associate
Téléphone direct: +41 58 658 56 63
lena.goetzinger@walderwyss.com

L'actuelle Loi suisse sur la protection des données (**LPD**) est en vigueur depuis 1993. Depuis lors, la digitalisation a considérablement modifié les modèles d'affaires, les risques pour les personnes concernées et les attentes en matière de protection des données. Dans l'EEE, le RGPD est applicable depuis mai 2018 et la Convention 108 du Conseil de l'Europe a été révisée. La LPD fait également l'objet d'une révision, à de nombreux égards sur le modèle du RGPD. Cela conduit à un renforcement des obligations et des risques pour les entreprises, tandis que la position du Préposé fédéral à la protection des données et à la transparence (**PFPDT**) a été considérablement renforcée.

Contrairement au RGPD, la révision de la LPD concerne toutes les entreprises qui sont domiciliées en Suisse ou dont le traitement a un impact ici - y compris les entreprises qui n'ont aucun contact avec les marchés étrangers. Il n'existe pratiquement pas de dispositions particulières pour les PME. Des mesures préparatoires ou de mise en œuvre sont donc nécessaires, non seulement pour les entreprises qui opèrent dans des secteurs réglementés, qui traitent des données particulièrement sensibles ou volumineuses ou qui sont bien connues du public.

Toutefois, une mise en œuvre n'est réussie et durable que si elle tient compte de la complexité de l'environnement et des risques et conditions-cadres de l'entreprise. Une approche « taille unique » est tout aussi malavisée qu'une mise en œuvre trop fortement focalisée sur les détails. Une approche pragmatique et axée sur les objectifs est essentielle.

Les nouveautés les plus importantes

La Loi sur la protection des données révisée (**révLPD**) a été adoptée par le Parlement le 25 septembre 2020. Cette révision nécessite également une révision des ordonnances pertinentes, en particulier de l'Ordonnance relative à Loi fédérale sur la protection des données (**OLPD**). Le début d'un processus de consultation sur la révision de l'OLPD (révOLPD) est actuellement prévu pour le milieu de l'année 2021. La révOLPD et la révLPD devraient toutes deux entrer en vigueur initialement vers le milieu de l'année 2022.

Certaines nouveautés auront un effet dans la pratique, mais sont de moindre importance au regard de la conformité à la loi de l'entreprise, par exemple sa limitation aux données des personnes physiques. Les points suivants, en revanche, sont d'une importance primordiale pour la mise en œuvre :

i. Les responsables du traitement et les sous-traitants doivent tenir un inventaire de leurs activités de traitement (« registre des activités de traitement »), par analogie avec l'obligation correspondante selon le RGPD.

ii. Les responsables du traitement peuvent nommer un conseiller à la protection des données, ce qui facilite le travail des analyses d'impact relatives à la protection des données (AIPD).

iii. Le révLPD prévoit un devoir d'information de principe lors de chaque collecte de données, qui ne s'applique plus seulement aux données sensibles. En revanche, aucune nouvelle exigence en matière de consentement n'est créée, même pour le profilage, par exemple

iv. Le droit de la protection des données exige que les risques pour les personnes concernées soient traités de manière appropriée. Cela implique notamment que le responsable du traitement tienne compte des risques dès la phase de planification des opérations de traitement et qu'il décide judicieusement de la manière dont il peut respecter la protection des données (« Privacy by Design »). Dans le cas d'un traitement plus délicat, l'évaluation des risques doit prendre la forme d'une AIPD et être documentée.

v. Dans certaines circonstances, les responsables de traitement traitant des données et basées à l'étranger doivent désigner un représentant en Suisse.

vi. Lorsque l'on travaille avec des clients, des fournisseurs et des partenaires, les droits et obligations en matière de protection des données doivent être réglés par contrat, par exemple par des accords entre les responsables du traitement et les sous-traitants.

vii. Les droits des personnes concernées sont renforcés, par exemple par le nouveau droit de recevoir une copie de certaines données sous un format électronique.

viii. La suppression ou l'anonymisation en temps utile des données personnelles reste importante

ix. Dans le cas de certaines infractions intentionnelles, les auteurs peuvent être sanctionnés par des amendes allant jusqu'à CHF 250'000. Dans certaines circonstances, les sociétés peuvent se voir infliger une amende allant jusqu'à CHF 50'000 à la place des personnes responsables. Il existe en outre des risques de responsabilité, des risques opérationnels et surtout des risques réputationnels dus à une éventuelle intervention du PFPDT.

Mise en œuvre

La mise en œuvre de la révLPD nécessite une planification anticipée. Cependant, les étapes centrales sont souvent réalisables avec relativement peu d'efforts. Une approche progressive est souvent possible et utile. Dans cette approche, certaines mesures sont prioritaires et d'autres mesures sont abordées dans une deuxième phase. Enfin, l'étendue de la mise en œuvre dépend également du fait que le RGPD ait déjà été implémentées ou non.

Clarification des besoins de mise en œuvre. Avant même de lancer un projet de mise en œuvre, l'entreprise - ou le groupe d'entreprises - doit déterminer le cadre juridique pertinent. Le RGPD et le droit national des États membres de l'EEE sont-ils applicables ? Des dispositions sectorielles supplémentaires s'appliquent-elles en Suisse ou à l'étranger, par exemple des dispositions relatives à la protection des secrets ou des dispositions du droit des assurances, du marché financier, de la santé ou de la recherche sur l'être humain ? L'entreprise agit-elle en tant qu'organisme privé ou (également) gouvernemental ? Dans ce contexte, on peut également décider si et dans quelle mesure l'application volontaire du RGPD est appropriée.

Registre des activités de traitement. Tant le RGPD que la révLPD exigent la création de « registres des activités de traitement », c'est-à-dire d'inventaires dans lesquels les différentes activités de traitement sont enregistrées (tant par les responsables du traitement que par les sous-traitants). Des exceptions peuvent s'appliquer aux PME. La création de registres au moins dans certains domaines - souvent soutenue par des solutions techniques appropriées - est généralement une première étape utile, car elle apporte un certain degré de clarté et aide à préparer l'entreprise et les personnes et fonctions responsables aux mesures d'exécution ultérieures. Si les entreprises ont déjà créé des registres des activités de traitement dans le cadre du RGPD, ceux-ci devraient également couvrir les exigences de la révLPD. La bonne tenue des registres des activités de traitement est tout aussi importante que leur création. Il est donc nécessaire de planifier les processus d'enregistrement des activités de traitement nouvelles ou modifiées.

Responsabilités internes. Les entreprises ont besoin d'une structure appropriée et des compétences nécessaires pour se conformer aux obligations en matière de protection des données, si une telle structure n'existe pas déjà. Si le RGPD s'applique, il peut être nécessaire de nommer un délégué à la protection des données si le RGPD ou le droit national l'exigent. Une telle obligation n'existe pas dans la révLPD, mais la désignation volontaire d'un conseiller à la protection des données peut offrir des avantages, comme notamment l'exemption de l'obligation de consulter le PFPDT (cf. art. 23 al. 4, révLPD).

Documentation complémentaire. Contrairement au RGPD, la révLPD ne comporte pas l'obligation générale du responsable du traitement de documenter de manière exhaustive le respect de la législation sur la protection des données. Une documentation est néanmoins nécessaire dans une certaine mesure. Compte tenu des principes généraux de traitement et des dispositions sectorielles spécifiques, il est également recommandé que le personnel soit formé dans les services concernés. Il est également utile, voire nécessaire, d'élaborer des lignes directrices, des guides et des fiches d'information. Si de telles mesures existent déjà dans le cadre du RGPD, elles doivent être adaptées à la révLPD - ce qui ne requiert qu'un effort limité.

Transparence, consentement et information. En plus du principe de transparence, la révLPD introduit un nouveau devoir d'information général et actif, dont

la violation est punie par la loi. Il est donc nécessaire de vérifier tout d'abord où et comment les données personnelles sont obtenues et quels sont les avis de protection des données déjà utilisés (par exemple dans les politiques de confidentialité ou les conditions générales). La révLPD fixe des exigences plus strictes à certains égards que le RGPD. Il convient également de vérifier si et où le consentement des personnes concernées est nécessaire ou utile et sous quelle forme il peut être obtenu. Une obligation d'obtenir le consentement peut également découler d'autres lois, par exemple dans le cas d'obligations de confidentialité.

Coopération avec des tiers. Dans le cadre de la coopération avec les fournisseurs et les clients, mais aussi en cas de flux de données intragroupe, les responsabilités et les obligations en matière de protection des données doivent être déterminées et faire l'objet d'un accord. Un accord – qui doit être écrit - doit également être conclu entre le sous-traitant et le responsable du traitement en vertu de la révLPD. En termes de contenu, cependant, les exigences ne vont pas aussi loin que le RGPD, dont les exigences sont devenues un standard. Des accords appropriés peuvent également être nécessaires dans le cas d'une responsabilité partagée et d'un échange de données entre responsables de traitement indépendants.

Sécurité des données et violations de la sécurité. Les entreprises doivent veiller à ce que le traitement des données soit conforme au principe de la protection des données par défaut, que la sécurité des données continue d'être garantie et que les violations de la sécurité des données soient détectées, communiquées en interne, portées à l'attention des organes supérieurs si nécessaire et, dans certaines circonstances, notifiées au PFPDT ou aux autorités compétentes ou aux personnes concernées. Cette obligation s'applique parallèlement à toute obligation légale spéciale d'annonce, par exemple, des institutions financières.

Droits des personnes concernées. Les droits des personnes concernées qui existent déjà aujourd'hui sont partiellement reformulés et complétés par le nouveau droit à la portabilité des données. Des processus doivent être mis en place à cette fin si les demandes des personnes concernées sont fréquentes. Même les entreprises qui ont déjà mis en œuvre le RGPD devraient vérifier cet aspect, car la révLPD diffère du RGPD sur quelques points importants.

Le respect de la protection des données nécessite une planification

La mise en œuvre du RGPD et de la révLPD n'est pas forcément coûteuse, mais nécessite une planification. Rien que pour des raisons de budgétisation et de reporting, une planification concrète est déjà nécessaire, ce également pour pouvoir réagir correctement aux changements et aux retards. Walder Wyss SA peut fournir un soutien grâce à une panoplie éprouvée d'instructions, de listes de contrôle et de modèles qui réduisent les efforts, le temps nécessaire et les coûts. Nous sommes également heureux de fournir aux entreprises un guide de mise en œuvre - n'hésitez pas à nous contacter.