SLVASSL

Schweizerischer Leasingverband
Association Suisse des Sociétés de Leasing

Aux membres de l'ASSL

Zurich, le 30 septembere 2020

Achèvement de la révision totale de la loi sur la protection des données suisse (LPD)

Mesdames et Messieurs

Après de longues tergiversations, le Parlement suisse a adopté la révision totale de la loi sur la protection des données suisse (LPD) après l'élimination des dernières divergences dans le cadre de son vote final du 25 septembre 2020. Par la présente, nous vous informons rapidement (encore une fois) sur la toile de fond de ce projet de loi et surtout sur ses principales nouveautés.

La révision totale doit adapter la loi sur la protection des données suisse obsolète (datant de 1992) à la situation sociale et technologique actuelle et se rapprocher des réglementations plus modernes de la législation européenne sur la protection des données (notamment UE-RGPD). Les quatre aspects suivants ont joué un rôle central dans ce contexte :

- Accroissement de la transparence et renforcement des droits des personnes concernées ;
- Encouragement de la prévention et de la responsabilité propre de ceux en charge du traitement des données ;
- Renforcement de la supervision de la protection des données :
- Développement des dispositions pénales.

Le message et l'avant-projet du Conseil fédéral laissaient craindre quelques durcissements légaux qui auraient entraîné une incertitude juridique pour de nombreuses entreprises et une charge de travail supplémentaire pour le traitement des données à caractère personnel. C'est la raison pour laquelle L'ASSL s'est engagée avec L'Union professionnelle suisse de l'automobile (UPSA) et ses associations partenaires, economiesuisse et l'Union suisse des arts et métiers usam, en faveur d'une mise en œuvre libérale et axée sur la pratique de la révision législative qui, d'une part, ne menace pas la décision de l'UE constatant le caractère adéquat et donc le transfert de données depuis l'UE vers la Suisse et, d'autre part, qui renonce à des réglementations strictes inutiles dépassant le cadre de l'UE-RGPD (sortes de « finitions suisses »). Nous avons en grande partie réussi

cet exercice comme par exemple concernant l'exception de tenue d'un registre de traitement et le droit d'accès et, tout du moins en partie, pour le profilage.

Dans un même temps, des **règles plus strictes** devront être respectées à l'avenir pour le traitement des données à caractère personnel. Il faut se pencher rapidement sur ces dernières pour contrôler votre concept de protection des données d'ici à l'entrée en vigueur de la loi révisée et pouvoir procéder à des modifications si besoin est (par exemple élaboration de déclarations de protection des données et le cas échéant de registres sur les activités de traitement, modification des processus de traitement des données, nomination d'un préposé à la protection des données, conclusion de contrats de sous-traitance pour le traitement des données, etc.).

Après l'arrivée à expiration du délai référendaire de 100 jours, le Conseil fédéral déterminera la date d'entrée en vigueur. Par conséquent, la loi sur la protection des données révisée (ci-après « **LPDrév** ») n'entrera pas en vigueur avant le 1er janvier 2022 d'autant plus que l'ordonnance correspondante (OLPD) doit encore être adaptée. Nous vous informerons à l'avance de la décision du Conseil fédéral.

Des nouveautés importantes

Veuillez noter que nous ne pouvons pas expliquer dans le détail toutes les nouvelles dispositions légales ou modifications dans le cadre de cette information destinée aux membres. Nous nous limitons donc à ce qui nous semble constituer les principales nouveautés par rapport au droit actuellement en vigueur :

- **Pas de protection des données des personnes morales :** tandis que la LPD actuelle s'applique aux données des personnes physiques et morales, la LPDrév limite son champ d'action aux données de personnes physiques, tout comme l'UE-RGPD.

- **Données personnelles particulièrement sensibles :** la LPDrév étend la liste des données considérées comme particulièrement sensibles et donc liées à des conséquences juridiques qualifiées (notamment obtention d'un accord, analyse d'impact relative à la protection des données personnelles, divulgation à des tiers et examen de la solvabilité). Les données génétiques et biométriques (par exemple empreintes digitales) identifiant sans équivoque une personne physique sont par exemple désormais également considérées comme des données particulièrement sensibles.

- **Profilage et profilage à risque élevé :** outre le profilage « usuel », un « profilage à risque élevé » doit être incorporé à la loi ce qui constituait la question la plus violemment contestée et la plus discutée de tout le projet. Pour finir, les deux chambres ont suivi les propositions de la conférence de conciliation qui prévoit de définir légalement le profilage à risque élevé et de le réglementer spécialement, contrairement à nos recommandations. Pour un profilage à risque élevé, une éventuelle autorisation requise doit être *explicite*. De plus, l'intérêt justifié du responsable du traitement et donc son motif justificatif à une atteinte à la personnalité disparaissent quand ses traitements des données comportent un profilage à risque élevé pour l'examen de la solvabilité.

On est en présence d'un profilage à risque élevé quand les données à caractère personnel sont traitées de manière automatisée et quand le regroupement des données permet « d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique ». La définition légale fait

l'objet d'une formulation très ouverte et il ne sera dans la pratique pas facile de faire la distinction avec un profilage « normal ». L'ordonnance va encore clarifier la question.

Quoi qu'il en soit, ce changement signifie que, pour effectuer un examen de solvabilité utilisant un profilage à risque élevé, il faut respecter tous les principes de traitement ou avoir un autre motif justificatif (notamment autorisation de la personne concernée).

- **Code de comportement :** la LPDrév permet notamment aux associations professionnelles, sectorielles et économiques, lorsqu'elles sont autorisées de par leurs statuts à défendre les intérêts économiques de leurs membres, à soumettre leur code de conduite au Préposé fédéral à la protection des données et à la transparence (PFPDT). Cette manière de procéder doit encourager le développement de l'auto-régulation et la responsabilité propre des responsables du traitement. Le PFPDT prend alors publiquement position sur ce code. Une prise de position positive ne permet pas de déduire de droits

Mais on peut toujours partir du principe qu'un comportement conforme au code ne risque pas d'entraîner de mesures administratives. De plus, les responsables du traitement respectant ce code peuvent dans certaines conditions renoncer à effectuer une analyse d'impact relative à la protection des données personnelles. Comme vous le savez déjà, l'ASSL soutient la « Charte de l'économie suisse pour une gestion responsable des données » (le code de conduite est consultable au lien suivant : https://www.economiesuisse.ch/fr/gestiondedonnees).

- **Registre de traitement des données :** tout comme l'UE-RGPD, la LPDrév prévoit une obligation de tenir un registre de tous les traitements de données effectués pour le responsable du traitement et le sous-traitant. Le registre en question doit au moins contenir les informations définies par la loi. Le Conseil fédéral prévoit des exceptions pour les entreprises employant moins de 250 collaborateurs et dont le traitement des données entraine un risque réduit d'atteinte à la personnalité des personnes concernées. Ces exceptions doivent encore être précisées dans l'ordonnance.

- **Sous-traitants :** selon la LPDrév, une relation de sous-traitance peut être justifiée par un contrat ou par la loi. Tout comme dans le droit en vigueur, la condition est que le sous-traitant traite les données comme le responsable du traitement le ferait lui-même. Comme dans l'UE, un transfert du traitement des données à un sous-traitant n'est désormais permis qu'avec l'approbation préalable du responsable du traitement afin que ce dernier conserve le contrôle (au moins indirectement) sur le traitement des données et afin que le responsable du traitement puisse s'assurer que le sous-traitant est en mesure de garantir la sécurité des données. Sinon, les changements sont minimes à ce niveau. Le contrat de sous-traitance n'est notamment toujours pas soumis à des dispositions formelles spéciales.

- **Protection des données dès la conception et par défaut :** comme l'UE-RGPD, la LPDrév contient des principes de protection dès la conception (« Privacy-by-Design ») et par défaut (« Privacy-by-Default »). Dès la conception du traitement des données (Privacy-by-Design), le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données, en particulier les principes de traitement. Il est par ailleurs tenu de garantir, par le biais de préréglages appropriés, par exemple des applications mobiles ou des sites Internet, que le trai-

tement des données personnelles est limité au minimum requis par la finalité poursuivie (Privacy-by-Default).

- **Extension des devoirs d'informer :** selon la LPDrév, les informations minimales suivantes doivent désormais être communiquées à la personne concernée lors de l'acquisition de données personnelles :

    - l'identité et les coordonnées du responsable du traitement ;
    - la finalité du traitement ;
    - le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises.

Lorsque des données personnelles sont communiquées à l'étranger, il faut également communiquer à la personne concernée le nom de l'État ou de l'organisme international auquel elles sont communiquées et, le cas échéant, les garanties prévues pour la protection des données personnelles.

- **Extension des devoirs de fournir des renseignements :** par rapport à la LPD en vigueur, la LPDrév prévoit des devoirs de fournir des renseignements élargis. Le devoir de fournir des renseignements ne se limite désormais plus aux informations minimales définies de manière exhaustive (qui comprennent désormais aussi des indications sur la durée de conservation, les transferts à l'étranger et les décisions individuelles automatisées) mais englobe les informations requises par la personne concernée pour faire valoir ses droits conformément à la LPDrév. Quoi qu'il en soit, les informations sur « les données personnelles traitées » doivent désormais également être communiquées « en tant que telles ». Cela clarifie le fait que le droit d'accès relevant de la protection des données ne constitue pas un droit à une édition ou publication d'actes.

- **Droit à la transférabilité des données :** la LPDrév prévoit un droit à la publication et la transmission des données (« portabilité des données »). Par conséquent, la personne concernée peut exiger du responsable du traitement, en règle générale gratuitement, la publication de ses données personnelles dans un format électronique courant ou leur transmission à un autre responsable du traitement si le responsable du traitement traite les données de manière automatisée et que les données ont été traitées avec l'accord de la personne concernée ou en lien direct avec la conclusion ou l'exécution d'un contrat.

- **Décision individuelle automatisée :** la LPDrév prévoit pour le responsable du traitement une obligation d'informer la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement des données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative. La personne concernée doit avoir la possibilité d'exposer son point de vue et peut exiger que la décision soit contrôlée par une personne physique. Cela ne s'applique pas lorsque la décision est en relation directe avec la conclusion ou l'exécution d'un contrat entre le responsable du traitement et la personne concernée, et que la demande de cette dernière est satisfaite ou lorsque la personne concernée a expressément accepté que la prise de décision soit automatisée.

En cas de décision exclusivement automatisée concernant la conclusion d'un contrat de leasing, le demandeur doit donc avoir la possibilité de prendre position et d'exiger qu'une personne physique

contrôle la décision sauf si la demande de leasing est approuvée ou que le demandeur a expressément accepté que la décision soit automatisée.

- **Analyse d'impact relative à la protection des données personnelles :** selon la LPDrév, le responsable du traitement a l'obligation d'effectuer une analyse d'impact relative à la protection des données personnelles quand un traitement des données est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. L'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. L'analyse d'impact relative à la protection des données personnelles contient une description du traitement envisagé, une évaluation des risques qui en découlent ainsi que les mesures adaptées pour prévenir lesdits risques. Des exceptions sont possibles dans certaines circonstances quand le responsable du traitement respecte un code de conduite.

- **Annonce des violations de la sécurité des données :** selon la LPDrév, les responsables du traitement annoncent dans les meilleurs délais au PFPDT les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Sous réserve de certaines exceptions, le responsable du traitement informe aussi la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige. Le sous-traitant annonce dans les meilleurs délais au responsable du traitement (pas au PFPDT et/ou à la personne concernée) tout cas de violation de la sécurité des données.

- **Sanctions :** selon la LPDrév, les personnes physiques peuvent désormais être sanctionnées par une amende pouvant atteindre CHF 250 000.00 (contre auparavant CHF 10 000.00 au maximum) notamment en cas de violation intentionnelle des devoirs d'informer ou de fournir des renseignements et de violation intentionnelle des devoirs de diligence. À l'avenir, le non-respect de la protection des données risque donc non seulement de nuire à la réputation des entreprises mais peut aussi entraîner des conséquences personnelles importantes pour le personnel en faute sur le plan pénal.

Webinaire

Nous attirons votre attention sur le webinaire de protection des données développé (dans toutes les langues) par l'ASSL et l'UPSAL et qui sera prochainement disponible sur le site Internet. Il doit vous donner un aperçu des principales bases légales de la protection des données et des (nouvelles) obligations pour le traitement des données avec des liens vers les documents types.

Quoi qu'il en soit, ce webinaire ne peut bien évidemment pas remplacer le conseil juridique qui sera nécessaire pour le contrôle et, le cas échéant, l'adaptation de vos concepts de protection des données.

Bien à vous

Prof. Dr. Cornelia Stengel
Geschäftsführerin

MLaw Luca Stäuble
Stv. Geschäftsführer