AGVS | UPSA
Auto Gewerbe Verband Schweiz
Union professionnelle suisse de l'automobile
Unione professionale svizzera dell'automobile

SLVASSL
Schweizerischer Leasingverband
Association Suisse des Sociétés de Leasing

La révision de la loi suisse sur la protection des données (LPD) est terminée

De nouvelles règles s'appliquent à partir du 1er septembre 2023

Par le biais de diverses informations aux membres depuis 2017, nous vous avons informés sur la révision totale en cours de la loi suisse sur la protection des données et des travaux de l'ASSL à ce sujet dans le cadre du projet commun avec l'UPSA. La révision de la loi suisse sur la protection des données (LPD) est terminée. Le 31 août 2022, le Conseil fédéral a publié l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) et décidé de l'**entrée en vigueur des nouvelles règles au 1er septembre 2023**.

L'ASSL et l'UPSA se sont engagées en faveur d'une révision de la loi sur la protection des données qui soit à la fois propice à l'économie et compatible avec l'UE. La loi et l'ordonnance qui l'accompagnent qui ont été décidées sont certes conformes à de nombreux égards aux règles de l'UE. Néanmoins, lors de l'examen et de la mise en œuvre de la nouvelle configuration de protection des données dans une entreprise, il convient de tenir compte de certaines spécificités suisses.

Les entreprises suisses ont désormais **un an pour mettre en œuvre les nouvelles règles** – aucune période transitoire (supplémentaire) n'est prévue.

Nous vous présentons ci-dessous une sélection des nouveautés qui devraient le plus vous concerner en tant que membres. Vous trouverez également en annexe une check-list des différentes tâches à accomplir pour la mise en œuvre progressive des nouvelles règles de protection des données dans votre entreprise.

1. Nouvelles désignations des rôles (art. 5, let. j et k nLPD)

Les nouvelles règles introduisent les notions de « responsable du traitement » et de « sous-traitant ». Pour comprendre les explications suivantes ainsi que le texte de loi lui-même, il est utile de connaître ces deux rôles. Est considérée comme **responsable** toute personne qui [...] détermine les finalités et les moyens du traitement de données personnelles, c'est-à-dire par exemple un employeur pour le traitement des données personnelles de ses employés ou un concessionnaire pour le traitement des données personnelles de ses clients. En revanche, est considéré comme **sous-traitant** celui qui [...] traite des données personnelles pour le compte du responsable du traitement, par exemple le stockage de données sur un serveur externe ou par des prestataires de cloud.

2. Profilage (art. 5 let. f. nLPD)

Une distinction est faite entre le « profilage » normal et le « profilage à risque élevé ». Le **profilage** désigne toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer, analyser ou prédire certains aspects personnels relatifs à une personne physique (art. 5 let. f nLPD). Le **profilage à risque élevé** implique en outre un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 5 let. g nLPD). Le profilage **ne requiert pas en soi de consentement**, même en cas de risque élevé. Il est toutefois important dans le contexte des devoirs d'informer, de l'obligation d'établir des procès-verbaux de journalisation et de l'analyse d'impact relative à la protection des données (voir ci-dessous).

3. Devoirs d'informer et de renseigner nettement plus étendus

Les nouvelles règles exigent que les personnes concernées soient notamment **informées** de la collecte de données personnelles, en communiquant toutes les informations nécessaires pour que les personnes concernées puissent faire valoir leurs droits et pour garantir un traitement transparent des données. Il s'agit notamment des coordonnées du responsable, de la finalité du traitement et, le cas échéant, des destinataires des données personnelles si celles-ci sont transmises (art. 19 nLPD). La violation intentionnelle de cette obligation est sanctionnée par le droit pénal.

Toute personne peut se **renseigner** et demander si des données personnelles la concernant sont traitées. Si c'est le cas, toutes les informations nécessaires pour lui permettre de faire valoir ses droits et pour garantir un traitement transparent des données doivent lui être communiquées. La loi contient une énumération en ce sens (art. 25 nLPD).

4. Décision individuelle automatisée (art. 21 nLPD)

Une décision individuelle automatisée est une décision qui est prise sans intervention humaine sur la base d'une analyse de données (p. ex. conditions telles que taux d'intérêt, durée du contrat, délais de paiement ou conclusion d'un contrat d'assurance ou de crédit, etc.) et qui entraîne une conséquence juridique pour la personne concernée ou l'affecte de manière significative.

La personne concernée doit être **informée** de cette décision individuelle automatisée et doit avoir la possibilité **d'exprimer son point de vue.** La personne concernée peut – si elle n'a pas donné son consentement explicite préalable à ce que la décision soit prise de manière automatisée – demander qu'une **vérification soit effectuée par une personne physique**.

Dans le cadre du droit d'accès, une personne concernée doit être informée de la logique sur laquelle repose une décision individuelle automatisée.

5. Obligations administratives

Les obligations administratives ont également été développées. Elles comprennent par exemple :

- La tenue d'un *registre des activités de traitement* (art. 12 nLPD). Un registre des activités de traitement est un inventaire qui contient les différentes activités de traitement de données effectuées dans l'entreprise. Les différentes finalités du traitement (par ex. ressources humaines, marketing, etc.) et leurs principales conditions-cadres sont saisies. Des exceptions s'appliquent aux entreprises de moins de 250 collaborateurs (art. 24 OLPD) ;

- La réalisation d'*analyses d'impact relatives à la protection des données* lorsqu'un traitement est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 22 nLPD) ;

- Les *devoirs d'annoncer* en cas de violation de la loi sur la protection des données (art. 24 nLPD et art. 15 OLPD) ;

- L'établissement de *procès-verbaux de journalisation* des traitements automatisés de données personnelles sensibles à grande échelle ou de profilage à risque élevé,

lorsque les mesures préventives prises ne permettent pas de garantir la protection des données (art. 4 OLPD) ; et

- La création d'un *règlement pour les traitements automatisés*. Celui-ci doit en outre être régulièrement mis à jour lorsque des données personnelles sensibles font l'objet d'un traitement automatisé à grande échelle ou d'un profilage à risque élevé (art. 5 OLPD).

6. Sécurité des données (art. 8 nLPD)

Des mesures techniques et organisationnelles (p. ex. droits d'accès, pseudonymisation) doivent être prises afin de garantir une sécurité adéquate des données. Cela implique également que les applications soient conçues, entre autres, de manière à ce que les données personnelles soient anonymisées par défaut et/ou effacées après un certain temps.

Si les données personnelles sont traitées par un sous-traitant, le responsable doit s'assurer que le sous-traitant est également en mesure de garantir la sécurité des données (p. ex. par le biais de contrats de sous-traitance pour le traitement des données).

En ce qui concerne la sécurité des données, il convient également de mentionner que « pendant toute la durée du traitement », il existe une obligation de vérifier et, le cas échéant, d'adapter les mesures prises et qu'une violation intentionnelle des exigences minimales en matière de sécurité des données est passible de sanctions.

7. Communication de données personnelles à l'étranger

Est notamment considéré comme une communication le stockage des données personnelles sur un système étranger (serveur, cloud), mais aussi un accès par une équipe d'assistance étrangère.

En principe, les données personnelles peuvent être communiquées à l'étranger si la législation de l'État tiers garantit une protection adéquate (art. 16, al. 1 nLPD). Les pays dans lesquels c'est le cas sont énumérés à l'annexe 1 de l'OLPD. En cas de communication de données personnelles à *d'autres* États, notamment aux États-Unis, l'application d'une disposition d'exception concrète ou la mise en œuvre de mesures de protection alternatives visant à garantir une protection adéquate des données sont requises (art. 16, al. 2, et art. 17 nLPD).

8. Sanctions

La nouvelle loi sur la protection des données prévoit des amendes pouvant aller jusqu'à CHF 250 000 en cas de violation de certaines obligations (art. 60 et suivants nLPD). Les actes et omissions intentionnels sont punissables, mais pas la négligence. Contrairement à l'UE, où les sanctions sont dirigées contre les entreprises, en Suisse, c'est en principe la personne physique responsable qui est passible de l'amende. L'entreprise elle-même ne peut être punie que d'une amende de CHF 50 000 au maximum si l'identification de la personne physique coupable d'une infraction au sein de l'entreprise ou de l'organisation entraînerait des frais d'enquête disproportionnés.

Nous vous recommandons de commencer rapidement à mettre en œuvre ces nouvelles réglementations afin que votre entreprise soit conforme à la LPD le 1er septembre 2023.

Septembre 2022