Révision de la loi fédérale sur la protection des données: principales modifications et éventuelles mesures à prendre quant aux nouvelles exigences

1. Introduction

Le 25 septembre 2020, le Conseil national et le Conseil des États ont approuvé le texte soumis au vote final de la loi sur la protection des données (LPD) révisée. Le délai référendaire de cent jours échu, le Conseil fédéral a fixé lors de sa séance du 31 août 2022 la date d'entrée en vigueur de la nouvelle loi au 1er septembre 2023. Le délai transitoire d'un an donne aux responsables de la protection des données dans l'économie suffisamment de temps pour prendre les mesures nécessaires afin d'appliquer la nouvelle législation.

La loi sur la protection des données révisée s'appuie beaucoup sur le Règlement général sur la protection des données (RGPD) de l'Union européenne, bien que des différences ponctuelles demeurent entre la législation suisse et la législation européenne. Les explications suivantes se rapportent uniquement à la loi fédérale révisée. Examiner si certains secteurs d'activité d'une entreprise suisse sont soumis au RGPD et quelles différences il y a dans le détail incombe à chaque entreprise. Si le RGPD s'applique, ses dispositions doivent être strictement respectées et mises en œuvre. Pour davantage de renseignements sur le RGPD et son application aux entreprises de transport suisses, voir Conseils pratiques concernant le RGPD (admin.ch).

Nous tenons enfin à signaler que le présent document fournit un aperçu de certaines nouveautés importantes de la LPD et sert d'aide pour prendre les éventuelles mesures nécessaires. Toutes les nouveautés ne sont pas indiquées. L'Union des transports publics ne garantit ni l'exhaustivité ni l'exactitude de ces informations.

2. Principales modifications de la LPD révisée

Le texte soumis au vote final est disponible **ici**.

Champ d'application à raison de la personne

La loi sur la protection des données révisée régit désormais uniquement le traitement de données personnelles concernant des personnes physiques (cf. art. 2 LPD révisée). La LPD actuelle s'applique en revanche aussi au traitement des données concernant des personnes morales (cf. art. 2 LPD).

Responsable du traitement et sous-traitant

On distingue nouvellement les rôles du responsable du traitement et du sous-traitant. Le responsable du traitement est la personne privée ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles (cf. art. 5, let. j LPD révisée). Le sous-traitant est la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement (cf. art. 5, let. k LPD révisée).

Profilage et profilage à risque élevé

Outre le profilage, la loi réglemente dorénavant le profilage à risque élevé. Celui-ci entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique (cf. art. 5, let. f et g LPD révisée). Le consentement exprès de la personne concernée est nécessaire pour le profilage à risque élevé. Il en va de même pour tout profilage effectué par un organe fédéral, peu importe si le risque élevé porte sur la personnalité ou les droits fondamentaux de la personne concernée (cf. art. 6, al. 7 LPD révisée).

Dählhölzliweg 12
CH-3000 Berne 6
info@utp.ch
www.utp.ch

Déclaration de fichiers

La LPD appelle «fichier» tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée (cf. art. 3, let. g LPD). Dans certains cas, les personnes privées sont tenues de déclarer leurs fichiers au préposé fédéral à la protection des données et à la transparence (PFPDT) (cf. art. 11a, al. 3 LPD). Cette obligation de déclaration au PFPDT disparaît dans la LPD révisée.

Protection des données dès la conception et par défaut

Le responsable du traitement est tenu – désormais dès la conception du traitement – de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données, en particulier les principes fixés à l'art. 6 LPD révisée (cf. art. 7, al. 1 LPD révisée, notion de «protection des données dès la conception»). De plus, le responsable du traitement est tenu de garantir, par le biais de préréglages appropriés (p. ex. sur les sites Internet et dans les applications), que le traitement des données personnelles soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement (cf. art. 7, al. 3 LPD révisée, notion de «protection des données par défaut»).

Conseiller à la protection des données

Les responsables du traitement privés peuvent nommer un conseiller à la protection des données. Ce dernier est l'interlocuteur des personnes concernées et des autorités chargées de la protection des données en Suisse. Il doit notamment former et conseiller le responsable du traitement privé dans le domaine de la protection des données et concourir à l'application des prescriptions relatives à la protection des données (cf. art. 10 LPD révisée).

Registre des activités de traitement

Les responsables du traitement et les sous-traitants doivent à l'avenir tenir chacun un registre de leurs activités de traitement (cf. art. 12, al. 1 LPD révisée). Les indications minimales que doivent contenir les registres figurent à l'art. 12, al. 2 et 3. Le Conseil fédéral prévoit des exceptions pour les entreprises qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées (cf. art. 12, al. 5 LPD révisée).

Devoir d'informer étendu

Jusqu'à présent, la personne concernée doit être informée activement de la collecte de données personnelles uniquement lorsqu'il s'agit de données sensibles ou de profils de la personnalité la concernant (cf. art. 14, al. 1 LPD). Dorénavant, le responsable du traitement informe la personne concernée de manière adéquate de la collecte de données personnelles, que celle-ci soit effectuée directement auprès de la personne ou non (cf. art. 19, al. 1 LPD révisée). Les indications minimales à communiquer sont réglées à l'art. 19, al. 2 LPD révisée. D'autres dispositions réglementent la collecte de données personnelles auprès de tiers et la communication de données à l'étranger à l'art. 19, al. 3 à 5 LPD révisée. L'art. 20 LPD révisée nomme les exceptions au devoir d'informer et ses restrictions.

Analyse d'impact relative à la protection des données personnelles

Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles (cf. art. 22 LPD révisée). L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. L'art. 22, al. 2 LPD révisée donne quelques exemples. Ce que doit contenir l'analyse d'impact et les conditions dans lesquelles on peut y renoncer figurent à l'art. 22, al. 3 à 5. Les situations lors desquelles le PFPDT doit être consulté au préalable sont indiquées à l'art. 23 LPD révisée.

Annonce des violations de la sécurité des données

Le responsable du traitement annonce 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 (cf. art. 24, al. 1 LPD révisée). Le contenu final de cette annonce est régi à l'art. 24, al. 2 LPD révisée. Le responsable du traitement informe la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige (cf. art. 24, al. 4 LPD révisée). Les exceptions sont réglées à l'art. 24, al. 5 LPD révisée.

Droit d'accès

Le droit d'accès a été adapté et précisé à certains égards dans la LPD révisée (cf. art. 25 ss LPD révisée). Désormais, la personne concernée a le droit à la remise et à la transmission des données la concernant pour autant que certaines conditions soient remplies (cf. art. 28 LPD révisée), bien que le responsable du traitement puisse refuser, restreindre ou différer la remise ou la transmission de données personnelles pour les mêmes motifs que ceux prévus à l'art. 26, al. 1 et 2 (cf. art. 29, al. 1 LPD révisée).

Évaluation de la solvabilité comme motif justificatif

Une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi. Les intérêts prépondérants de la personne qui traite des données personnelles entrent notamment en considération si les données personnelles sont traitées dans le but d'évaluer le crédit d'une autre personne (cf. art. 13, al. 1 et 2, let. c LPD). Ces dispositions ont été précisées dans la LPD révisée. Les données ne doivent par exemple pas dater de plus de dix ans (cf. art. 31, al. 2, let. c LPD révisée).

Compétences de l'autorité de surveillance

Le PFPDT obtient de nouvelles compétences dans la loi révisée. Désormais, le PFPDT ouvre une enquête d'office ou sur dénonciation si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données (cf. art. 49 LPD révisée). Lorsque les personnes impliquées ne respectent pas leur obligation de collaborer, le PFPDT peut prendre diverses mesures (cf. art. 50 LPD révisée). De plus, si des dispositions de protection des données sont violées, le PFPDT peut ordonner des mesures administratives contraignantes alors qu'il ne peut jusqu'ici qu'émettre des recommandations (cf. art. 51 LPD révisée).

Sanctions relevant du droit pénal

Les sanctions relevant du droit pénal ont été durcies et le catalogue des infractions complété. Dorénavant, les personnes physiques peuvent être punies (parfois sur plainte) d'une amende de 250 000 francs au plus si elles violent certaines dispositions (cf. art. 60 ss LPD révisée). Face à des infractions commises dans une entreprise, l'autorité peut renoncer à poursuivre la personne physique et condamner l'entreprise au paiement de l'amende à sa place, lorsque l'amende entrant en ligne de compte ne dépasse pas 50 000 francs et que l'enquête rendrait nécessaires à l'égard des personnes punissables des mesures d'instruction hors de proportion avec la peine encourue (cf. art. 64 LPD révisée).

3. Mesures à prendre à l'égard des nouvelles exigences de la loi sur la protection des données révisée

Organiser l'entreprise

Premièrement, il faut clarifier qui est responsable de la protection des données (éventuellement nommer un conseiller à la protection des données) et comment ce domaine est réglementé, soit comment le respect des dispositions relatives à la protection des données est assuré. Ce domaine doit être contrôlé régulièrement et, le cas échéant, adapté. Il est possible de prévoir des audits et d'élaborer ou de modifier des directives internes.

Identifier et documenter les opérations de traitement des données

Au sein de l'entreprise, les opérations de traitement doivent être définies, analysées, documentées, comparées aux nouvelles dispositions et, le cas échéant, adaptées. Cela vaut également pour la transmission de données à l'étranger. Il est important de noter que le terme «traitement» comprend toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données (cf. art. 5, let. d LPD révisée).

Désormais, l'entreprise doit tenir un registre des activités de traitement des données personnelles. Les indications minimales qu'il doit contenir figurent à l'art. 12 LPD révisée. Pour les entreprises qui emploient moins de 250 collaborateurs, le Conseil fédéral prévoit des exceptions à l'obligation de tenir ledit registre (ces exceptions n'ont pas encore été formulées). Or, même dans ce cas, les opérations de traitement des données doivent être documentées. Étant donné que la tenue d'un registre des activités de traitement peut être synonyme de charges non négligeables, il est recommandé de se pencher sur ce travail tôt, soit avant l'entrée en vigueur de la loi révisée. Cela permet de mettre en œuvre les mesures éventuellement nécessaires à temps.

Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement procède en sus au préalable à une analyse d'impact relative à la protection des données personnelles (cf. art. 22 LPD révisée).

Définir des procédures appropriées

Il y a lieu d'examiner si des procédures efficaces permettant de garantir le respect des dispositions de la LPD s'appliquent déjà ou si celles-là doivent encore être établies. Les cas de violation de la sécurité des données doivent être annoncés dans les meilleurs délais. Dans certains cas, il peut même être requis de les annoncer au plus vite au PFPDT (cf. art. 24 LPD révisée). Les collaborateurs doivent être sensibilisés à la problématique de la protection des données et, au besoin, y être formés.

Par ailleurs, toute personne peut demander à l'entreprise si des données personnelles la concernant sont traitées (cf. art. 25, al. 1 LPD révisée). Cette demande de renseignements doit en règle générale être satisfaite dans un délai de trente jours (cf. art. 25, al. 7 LPD révisée). Les réponses aux demandes de renseignements doivent donc être garanties dans les temps et de manière complète. Il en va de même des demandes déposées par les autorités.

Les principes relatifs au traitement de données personnelles visés à l'art. 6 LPD révisée doivent être garantis par des procédures (techniques) appropriées. Les données doivent par exemple être détruites/supprimées ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement (cf. art. 6, al. 4 LPD révisée).

Examen et mise à jour des documents

L'ensemble des documents ayant trait au traitement de données personnelles doivent être examinés quant aux prescriptions légales de la LPD révisée et, si nécessaire, modifiés (en accord avec les éventuels partenaires contractuels). Cela concerne en particulier les déclarations de protection des données et les contrats conclus avec les sous-traitants (p. ex. entreprise IT qui traite les données et y a accès sur mandat de l'entreprise).

Mesures techniques et sécurité des données

L'entreprise est tenue de mettre en place, dès la conception, des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données (cf. art. 7, al. 1 LPD révisée). En ce qui concerne la sécurité des données, des mesures techniques et organisationnelles doivent être prises si nécessaire. Ces mesures doivent garantir une sécurité des données adaptée au risque existant et la confidentialité, la disponibilité et le caractère complet des données personnelles.