economiesuisse

Protection des données: tour d'horizon de la nouvelle loi

Le Parlement a adopté la nouvelle loi sur la protection des données en automne 2020. Le délai référendaire a expiré en janvier 2021 sans qu'un référendum ait été lancé. Les travaux relatifs à l'ordonnance d'exécution (OLPD) étant encore en cours, il faut s'attendre à ce que la nouvelle loi entre en vigueur au second semestre 2022.

Il est recommandé aux entreprises suisses de se familiariser dès aujourd'hui avec la nouvelle loi et ses exigences et d'adapter leur dispositif de protection des données, en particulier en ce qui concerne leurs dispositions relatives à la protection des données et contrats. economiesuisse répond aux questions les plus pressantes en collaboration avec deux avocats, Me Cornelia Stengel et Me Luca Stäuble, afin de signaler aux entreprises suisses les mesures à prendre en lien avec l'entrée en vigueur de la nouvelle loi sur la protection des données (LPD).

Le présent tour d'horizon a pour seul but d'informer et de sensibiliser les personnes intéressées. Il ne remplace pas un conseil juridique. economiesuisse ne pourra être tenue pour responsable des actions ou omissions consécutives à la lecture de cet article.

FAQ

1) Quels sont le but et le champ d'application de la nouvelle loi (nLPD)?

La nouvelle loi (nLPD) vise à protéger la personnalité et les droits fondamentaux des personnes physiques établies en Suisse et dont les données font l'objet d'un traitement par des privés (sociétés privées) ou par l'État. Les données des personnes morales ne seront plus protégées. L'idée sous-jacente est d'offrir aux personnes concernées une transparence accrue et ainsi de renforcer leurs droits sur leurs propres données («autodétermination informationnelle»). La nouvelle loi vise aussi à promouvoir les mesures de prévention et la responsabilité individuelle des responsables du traitement de données. Pour ce faire, la loi renforce la surveillance de la protection des données et développe les dispositions pénales. Elle instaure également de nouveaux devoirs pour les entreprises, notamment en cas de collecte, de perte ou d'utilisation abusive de données personnelles.

2) Où la nouvelle loi s'applique-t-elle?

Bien que la nLPD s'applique sur le territoire de la Suisse, elle a également une portée extraterritoriale puisqu'elle s'applique aux états de fait qui se produisent à l'étranger et qui déploient des effets en Suisse (art. 3). Autrement dit, si le processus de traitement de données personnelles a lieu hors de Suisse, mais qu'il concerne des personnes physiques établies en Suisse et produit des effets en Suisse (ce critère devrait être précisé dans l'ordonnance), le responsable du traitement des données en question est tenu de respecter la nouvelle législation suisse. Il doit en outre nommer, à certaines conditions, un représentant légal en Suisse (art. 14 et 15 nLPD).

Exemple: une entreprise a son siège à l'étranger et traite des données de personnes physiques établies en Suisse depuis l'étranger. Dans ce cas, il faut évaluer chaque situation. La nLPD s'applique si le traitement de données en Suisse est «sensible». Le RGPD examine, par exemple, si des données sont traitées en vue de concevoir une offre de biens ou de services destinées à des personnes au sein de l'UE.

3) En quoi une révision de la loi actuelle était-elle nécessaire?

La loi suisse sur la protection des données actuelle date de 1992. Depuis, la collecte et l'utilisation de données personnelles croissent à mesure que l'économie et la société se numérisent. À l'échelle mondiale et en particulier au sein de l'UE, la protection des données a été considérablement renforcée et les organisations internationales ont durci leurs normes minimales en la matière. Pour la Suisse, il était donc nécessaire d'adapter sa loi de 1992 aux nouveaux modes de consommation (achats en ligne, réseaux sociaux, etc.), aux développements technologiques (numérisation, intelligence artificielle, etc.) et aux normes internationales.

En adoptant son règlement général sur la protection des données (RGPD), l'Union européenne a mis en place un nouveau standard à l'échelle internationale. Entré en vigueur le 25 mai 2018, ce règlement fait parler de lui dans le monde entier en raison de sa portée extraterritoriale. De nombreuses entreprises suisses tombent dans le champ d'application du RGPD, en raison de leur orientation sur les marchés de l'UE ou de l'EEE. À cela s'ajoute que le RGPD prévoit que des données puissent être transférées vers un autre État uniquement si celui-ci présente un

niveau de protection des données «adéquat» du point de vue de l'UE. Une circulation des données fluide en provenance de l'UE est particulièrement importante pour des pays comme la Suisse, qui entretiennent des relations économiques très étroites avec l'UE.

Un objectif important de la révision de la LPD était donc d'élaborer une solution coordonnée au niveau international – «équivalente» aux yeux de l'UE – qui favorise les développements technologiques en lien avec l'économie des données et qui, en même temps, n'abandonne pas les atouts de la législation actuelle.

La nouvelle loi développe notamment les obligations en matière d'information et les droits des personnes concernées. Elle règle également ce qu'on appelle le «profilage». Ce dernier couvre tout genre de traitement automatisé de données personnelles en vue d'évaluer, d'analyser ou de prédire le comportement d'une personne physique (en particulier le rendement au travail, la situation économique, la santé, les intérêts, la localisation, par exemple). Des conséquences juridiques plus strictes ne s'appliquent qu'en cas de profilage présentant un risque élevé pour la personnalité de la personne concernée.

La Suisse dispose-t-elle d'un niveau de protection des données «adéquat» du point de vue de l'UE?

La Suisse est un «pays tiers» du point de vue de l'UE. Pour que le transfert de données vers un pays tiers soit possible, une décision de la Commission européenne relative à l'adéquation du dispositif suisse est nécessaire. La Suisse dispose d'une telle décision, mais celle-ci se fonde sur l'ancienne législation européenne. L'UE examine actuellement si la nouvelle LPD est également adéquate au regard du RGPD. Avec sa révision, la Suisse a normalement créé les conditions permettant à l'UE d'accorder l'adéquation. En raison d'une récente jurisprudence de l'UE sur la circulation de données vers des pays tiers, mais probablement aussi pour des raisons politiques, la décision annoncée pour 2020 a été reportée.

Enfin, il ne faut pas oublier que la modernisation du droit suisse s'inscrit dans un contexte international où les citoyens et les consommateurs dans le monde entier exigent une meilleure protection de leurs données personnelles et un contrôle accru sur ces données. Cette tendance ne s'observe pas uniquement dans l'UE, mais dans de nombreux pays, dont le Japon. La Californie a durci sa législation en matière de protection des données, en se fondant en partie sur la norme européenne.

4) Quand la nouvelle loi (nLPD) entrera-t-elle en vigueur?

Selon toute vraisemblance, la nLPD devrait entrer en vigueur au second semestre 2022. Dans la mesure où les travaux entourant les ordonnances ne sont pas terminés (consultation prévue en juin 2021), cette période n'a pas encore été confirmée et certaines sources tablent sur une entrée en vigueur plus tardive. Cela dit, la loi ne prévoit pas de période de transition, aussi les entreprises doivent-elles procéder aux ajustements nécessaires rapidement.

5) Dans quels domaines la nouvelle loi suisse va-t-elle plus loin que le RGPD européen?

La nouvelle LPD s'inspire du RGPD, mais présente quelques particularités. Dans la plupart des cas, la loi suisse est moins formaliste et a des exigences moindres par rapport au RGPD. Il y a cependant certains points où la nouvelle loi suisse sera plus stricte que le RGPD. Il s'agit notamment du champ d'application matériel (art. 2 nLPD), du devoir d'information lors de la collecte de données personnelles (art. 19 nLPD), des amendes pour les personnes physiques (art. 60 ss. nLPD) et de la définition des données personnelles particulièrement sensibles.

6) La nouvelle loi exclut-elle les PME? Seules les grandes entreprises seront-elles concernées?

Non. Toutes les entreprises, sans exception, sont concernées par la nouvelle LPD. Quelle que soit sa taille, une entreprise possède nombre de données sur ses clients, partenaires, fournisseurs et collaborateurs. Avec la numérisation de l'économie, la quantité de données à traiter par les entreprises, PME comprises, ira grandissant. Toutes les entreprises doivent se préparer à l'entrée en vigueur de la nouvelle loi. Cette loi s'alignant sur les standards européens, cela est d'autant plus vrai pour les entreprises suisses qui, dans le cadre leurs activités, n'ont pas encore adapté leur dispositif de protection des données au RGPD.

De plus, il convient de tenir compte du fait que la criminalité dans l'espace numérique est en constante augmentation. Le nombre de cyberattaques augmente et aucune entreprise n'est à l'abri. Or la nouvelle loi sur la protection des données impose aux entreprises de prendre les mesures organisationnelles et techniques nécessaires pour garantir la sécurité des données et éviter autant que possible leur utilisation abusive.

7) Que devront faire les entreprises pour se mettre en conformité?

Toute entreprise doit se préparer à l'entrée en vigueur de la nouvelle loi. Un recensement des données personnelles traitées au sein de l'entreprise et une évaluation des risques sont nécessaires pour déterminer les exigences de mise en conformité. Les travaux nécessaires pour la mise en conformité peuvent être identifiés au moyen d'une analyse des lacunes (comparaison de l'état actuel et de l'objectif). Les exigences de mise en conformité sont plus élevées, par exemple, lorsque:

- Les entreprises traitent un grand volume de données personnelles. Exemple: Des sociétés spécialisées dans la vente en ligne ou dans l'import/export ont un portefeuille de clients important générant un volume de données personnelles conséquent.
- Les entreprises traitent des données personnelles particulièrement sensibles (au sens de l'art. 5 nLPD). Exemple: Les entreprises traitant des données personnelles relatives aux opinions politiques, religieuses, à la santé, aux données génétiques, raciales, à l'aide sociale, aux poursuites, au profilage, etc. sont concernées.

Dans ces cas, les exigences relatives au traitement licite des données personnelles ou le risque de violation des droits de la personnalité sont plus élevés que dans le cas d'entreprises traitant les données d'un nombre limité de

collaborateurs, de fournisseurs, de clients, etc.

Ce travail de mise en conformité nécessitera, selon les cas et le volume de données personnelles traitées, le développement d'une certaine expertise ou le recours à des experts et l'établissement de procédures internes pour répondre aux exigences de la loi. Il ne faut pas sous-estimer les ressources matérielles (logiciels de gestion de données, etc.), humaines (nommer un responsable des questions relatives à la protection des données, etc.) et le temps qui doivent y être consacrés.

Selon l'ampleur de la mise en conformité, les entreprises sont vivement encouragées à faire appel aux services d'experts en informatique et d'avocats ainsi qu'aux formations proposées par les Chambres de commerce.

8) Pourquoi est-il important de se préparer dès maintenant?

Exception faite de certaines obligations, la nouvelle loi ne prévoit pas de délai de transition pour se mettre en conformité. Ainsi, une grande partie des devoirs des entreprises inscrits dans la loi s'appliqueront dès l'entrée en vigueur de la nLPD. Il est important et recommandé de se préparer bien à l'avance et d'identifier dès à présent les éventuelles mesures à prendre. Ainsi, afin de s'assurer qu'une protection efficace des données sera en place lorsque la nLPD entrera en vigueur, certaines actions peuvent d'ores et déjà être entreprises (développer l'expertise interne en temps utile, élaborer des directives internes et adapter des documents tels que les déclarations en matière de protection des données et les contrats avec des partenaires et des responsables du traitement des données).

9) Quelles sont les principaux changements par rapport à la loi actuelle?

La nouvelle loi introduit de nouvelles obligations pour les entreprises. Les principales sont:

- mettre en place des mesures techniques et organisationnelles afin que le traitement des données respecte les prescriptions de protection des données par défaut, en particulier afin que les principes établis pour le traitement soient respectés et que celui-ci soit limité au minimum nécessaire pour atteindre l'objectif visé (art. 7 nLPD);
- établir et tenir un registre des activités de traitement des données. Les entreprises de moins de 250 collaborateurs bénéficient ici d'une exception, mais seulement si leur traitement de données comporte un faible risque d'atteinte à la personnalité des personnes concernées (cela sera précisé dans l'ordonnance, art. 12 nLPD);
- notifier le préposé fédéral à la protection des données et à la transparence (PFPDT) et la personne concernée en cas de violation de la sécurité des données (art. 24 nLPD);
- effectuer une analyse d'impact relative à la protection des données personnelles lorsque le traitement des données présente un risque élevé (art. 22 nLPD);
- informer en cas de collecte de données et indiquer le nom du ou des États en cas de communication à l'étranger (art. 19 nLPD). Sur ce point, la nLPD est plus stricte que le RGPD;

- informer en cas de décision individuelle automatisée – c'est-à-dire une décision prise à l'égard d'une personne, par le biais d'algorithmes appliquée à ses données personnelles sans qu'aucun être humain n'intervienne dans le processus (art. 21 nLPD).

10)) Quels sont les nouveaux droits des personnes privées?

L'objectif principal de cette loi est de renforcer la transparence et la protection des données personnelles des personnes concernées. Dans cette optique, les personnes privées bénéficieront des nouveaux droits suivants:

- le droit d'être informé du traitement de ses données personnelles (art. 25-27 nLPD);
- le droit à la remise ou à la transmission des données personnelles (portabilité des données) (art. 28 et 29 nLPD)
- le droit de ne pas faire l'objet d'une décision individuelle automatisée – c'est-à-dire une décision prise à l'égard d'une personne, par le biais d'algorithmes appliquée à ses données personnelles sans qu'aucun être humain n'intervienne dans le processus (art. 21 nLPD).

11) Quels sont les autres changements par rapport à la loi actuelle?

Les autres changements par rapport à la loi actuelle sont les suivants:

- Données personnelles: Cette notion est désormais réduite puisqu'elle ne comprend plus les données des personnes morales et exclut ces dernières du champ de protection de la LPD (art. 1 et art. 5, let. a nLPD).
- Données personnelles sensibles: Elles incluent désormais les données génétiques et biométriques (permettant une identification unique) (art. 5, let. c nLPD).
- Responsable du traitement: Il correspond au «maître du fichier» actuel et au «responsable du traitement» selon le RGPD. Il s'agit d'une personne privée (souvent une entreprise) ou d'un organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles (art. 5, let. j nLPD).
- Extraterritorialité: Extension du champ d'application de la nLPD aux états de fait qui se produisent à l'étranger et qui déploient des effets en Suisse (art. 3, al. 1 nLPD).
- Nomination d'un représentant en Suisse pour des entreprises étrangères: Cette obligation s'applique lorsqu'un responsable du traitement privé a son siège ou son domicile à l'étranger et que celui-ci effectue un traitement de données personnelles concernant des personnes en Suisse et que d'autres conditions sont remplies (art. 14 f. nLPD).

12) Quels sont les risques encourus en cas de non-respect de la loi?

En cas de non-respect de la loi, les contrevenants risquent une amende allant jusqu'à 250 000 francs. Contrairement au RGPD, les sanctions prévues par la nLPD ne sont pas dirigées contre l'entreprise fautive, mais contre la personne physique en charge de la protection des données (directeur ou membre du conseil

d'administration, par exemple). Seul un comportement (pouvant être) intentionnel est sanctionné (art. 60 ss. nLPD).

13) Quels sont les enjeux pour les entreprises?

Ignorer la (nouvelle) loi sur la protection des données peut avoir des conséquences non seulement pour le responsable au sein d'une entreprise, mais aussi pour l'entreprise elle-même, en particulier sa réputation. Le préposé fédéral à la protection des données (PFPDT) peut intervenir et prendre des mesures administratives (ordonner la modification, la suspension ou la cessation d'un traitement ou l'effacement de données personnelles, par exemple).

14) Comment se préparer aux changements?

Il est tout d'abord nécessaire de s'y préparer dès que possible, et ce à l'aide d'une analyse des lacunes afin de s'adapter étape par étape à ce nouveau régime réglementaire. Selon la taille de l'entreprise, cela peut prendre plusieurs mois. Des solutions pragmatiques sont néanmoins de rigueur, c'est-à-dire qu'il faut commencer par mettre en œuvre les exigences minimales de la loi (un registre, l'obligation d'informer, etc.).

15) Comment définir un plan d'action?

Un plan d'action devrait reposer sur les trois piliers suivants: sécurité informatique, aspects juridiques et gouvernance des données. Concernant le dernier point, economiesuisse a mis à disposition une charte de l'économie suisse pour une gestion responsable des données. Au besoin, les entreprises devraient faire appel à des professionnels en sécurité informatique et protection des données pour élaborer en détail des programmes de conformité qui répondent aux nouvelles obligations pour les entreprises.

16) Quels principes retenir? Et quelles actions sont requises?

Sans entrer dans les considérations techniques, juridiques et informatiques d'une mise en conformité avec la nLPD, un plan d'action pragmatique devrait retenir les principes suivants:

1. **Un état des lieux global est primordial**
   Les entreprises devront être en mesure de répondre à tout moment à toute demande d'information, c'est-à-dire qu'en cas de collecte de données personnelles, elles doivent fournir des informations sur l'identité du responsable du traitement, la finalité du traitement, les éventuels destinataires des données, etc. Elles doivent aussi être en mesure de respecter les droits des personnes concernées, pour fournir à une personne concernée des informations sur le traitement de ses données personnelles. Cela suppose que les entreprises sachent quelles données personnelles sont traitées et à quelles fins, si ces données sont communiquées à d'autres pays et à d'autres personnes, etc. Par conséquent, les entreprises doivent commencer par faire un état des lieux

de toutes les données traitées. Le nouveau registre obligatoire peut servir de point de départ. Un tel état des lieux est un effort collectif de tous les collaborateurs impliqués dans le traitement de données personnelles.

2. **Évaluer les risques**
   Plus le volume de données personnelles traitées par une entreprise est important et plus les données personnelles sont sensibles, plus les exigences de conformité en matière de protection des données sont élevées et plus les sanctions potentielles et les atteintes à la réputation en cas de non-respect sont importantes (cf. question 6).
3. **Sensibiliser**
   Quelle que soit la taille de l'entreprise: tous les collaborateurs, de l'apprenti au chef d'entreprise, doivent être sensibilisés aux enjeux de la protection des données. Réceptionniste, chargé de projets, responsable des ressources humaines, consultant, indépendant, chef d'entreprise – des collaborateurs à tous les échelons d'une entreprise traitent régulièrement des données personnelles et en assument la responsabilité sur le plan pénal. Exemple: Un réceptionniste tient un registre des visiteurs d'une entreprise. En collectant et en archivant les noms et prénoms des personnes qui viennent dans l'entreprise, celui-ci traite déjà des données personnelles.
4. **Transparence et information**
   La transparence en matière de traitement des données reste un principe important avec la nouvelle LPD. Il y a aussi l'obligation d'information en cas de collecte de données. Le responsable du traitement est tenu d'informer les personnes concernées de divers aspects du traitement de données. L'établissement et la mise à jour de la déclaration en matière de protection des données sont essentiels en vue de l'entrée en vigueur de la nLPD (sur le site web de l'entreprise, mais aussi dans la correspondance).
5. **Sécurité informatique**
   Les entreprises doivent s'assurer que la sécurité des systèmes informatiques de l'entreprise et des applications logicielles répond aux exigences de la nouvelle loi. Cela comprend des mesures techniques et organisationnelles visant à prévenir les cyberattaques, le vol de données et autres pertes de données.
6. **Organisation et procédures internes**
   Afin de répondre conformément aux exigences de la nouvelle loi, aux éventuelles sollicitations externes (demandes d'information ou d'effacement des données personnelles d'un client) ou aux incidents impliquant la fuite, la perte ou l'utilisation abusive de données personnelles, il convient d'établir des procédures internes adaptées à la structure de chaque entreprise. Selon l'incident, ces procédures doivent définir quel(s) collaborateur(s) (suppléants inclus) doivent prendre quelle(s) mesure(s) et dans quel(s) délai(s). Exemple: dans le cas d'une violation de la sécurité des données, les procédures doivent établir les situations et critères permettant d'évaluer si un incident doit être signalé aux autorités. Ces procédures doivent en outre comporter des explications claires indiquant quel collaborateur doit signaler l'incident, dans quel délai, sous quelle forme et à quelle autorité. Ce genre de procédures peut prendre la forme de listes de contrôle (check-lists).
7. **Établir un registre des activités**
   La nLPD prévoit que le responsable du traitement et le sous-traitant doivent chacun tenir un registre de leurs activités. Cette obligation

concerne toutes les entreprises. Le Conseil fédéral peut toutefois prévoir des exceptions pour les entreprises de moins de 250 collaborateurs (art. 12, al. 2 nLPD). Ces exceptions seront précisées dans l'ordonnance, dont le projet est toujours en cours d'élaboration. L'établissement de tels répertoires suppose que tous les traitements de données personnelles au sein d'une entreprise soient identifiés et systématiquement rassemblés. En particulier dans des cas où un tel registre n'est pas encore tenu et où de nombreuses opérations différentes sont effectuées, cette procédure implique un travail considérable et doit donc être démarrée à un stade précoce.

8. **Révision des contrats**
   Au vu des changements qui s'opéreront avec la nouvelle loi et d'ici son entrée en vigueur, les entreprises devraient examiner – et si nécessaire, adapter – les contrats passés avec leurs clients, fournisseurs, prestataires de services mais également avec leurs collaborateurs. Il faut s'y prendre à temps. Une mise en œuvre rapide est également judicieuse, car il faut s'attendre à ce que de nombreux partenaires contractuels exigent dans les mois à venir des contrats – ou adaptations aux contrats déjà existants – incluant des clauses conformes à la nouvelle loi sur la protection des données.
9. **Rester informés**
   Pour comprendre les implications de la mise en conformité selon la nLPD, il est nécessaire de pouvoir assimiler les enjeux et les implications concrètes de la nouvelle loi sur les processus de travail. Informez-vous en consultant les sites des autorités de protection des données (PFPDT), des blogs et des revues spécialisés et participez aux différentes formations (proposées par des Chambres de commerce, par exemple).