economiesuisse

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

La révision de la loi suisse sur la protection des données (LPD) est achevée. Les nouvelles règles et les dispositions d'exécution contenues dans la nouvelle ordonnance sur la protection des données (OPDo) et la nouvelle ordonnance sur les certifications en matière de protection des données (OCPD) entrent en vigueur le 1er septembre 2023. Aucune période de transition n'est prévue.

Il est recommandé aux entreprises suisses de se familiariser au plus vite avec la nouvelle loi et ses exigences et d'adapter leur dispositif de protection des données, en particulier leurs dispositions relatives à la protection des données et leurs 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.

Le présent tour d'horizon a pour seul but d'informer et de sensibiliser les personnes intéressées. Il ne remplace toutefois pas un conseil juridique. economiesuisse ne pourra être tenue pour responsable pour les 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) 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 prennent de l'ampleur 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 personnelles puissent être transférées vers un État tiers 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 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. Toutefois, en révisant la LPD, la Suisse devrait avoir créé les conditions nécessaires pour que la Commission européenne continue de qualifier

la loi suisse sur la protection des données (révisée) d'adéquate. La (nouvelle) décision quant à l'adéquation est actuellement en attente.

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 d'ailleurs pas uniquement dans l'UE, mais dans de nombreux pays, dont le Nouvelle-Zélande. La Californie a durci sa législation en matière de protection des données, en se fondant en partie sur la norme de l'UE.

3) 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 (principe des effets) puisqu'elle s'applique à des états de fait qui se produisent à l'étranger et 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, le responsable du traitement des données en question est tenu de respecter la nLPD. Il doit en outre nommer, à certaines conditions, un représentant légal en Suisse (art. 14 et 15 nLPD).

Exemple: Une entreprise ayant son siège à l'étranger traite des données de personnes physiques établies en Suisse depuis l'étranger. Dans ce cas, il faut évaluer chaque situation. La nLPD s'applique que le traitement de données soit «sensible» ou non en Suisse – cela devrait déjà être le cas en règle générale lorsque des données sont traitées pour un certain nombre de personnes se trouvant en Suisse. Le RGPD, pour sa part, se fonde – pour autant qu'il n'y ait pas de bureau dans l'UE – sur le fait de savoir si le traitement des données est lié à l'orientation «manifestement intentionnelle» de l'offre de biens ou de services vers des personnes dans l'UE (la boutique en ligne est orientée dans ce sens, par exemple) ou à une observation des comportements en relation avec des personnes dans l'UE (utilisation de technologies de webtracking, par exemple). Dès lors, la portée géographique de la nouvelle réglementation suisse est encore plus large que celle du RGPD.

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

Le 31 août 2022, le Conseil fédéral a publié l'ordonnance sur la protection des données (OPDo) et fixé l'entrée en vigueur des nouvelles règles au 1er septembre 2023. Sachant que la loi ne prévoit pas de période de transition, c'est le bon moment pour se pencher sur la mise en œuvre des adaptations nécessaires.

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. Ainsi, le principe selon lequel le traitement de données personnelles est autorisé dans la mesure où ses principes sont respectés reste

valable (art. 6 nLPD). Contrairement à l'UE, il n'est donc pas nécessaire de disposer d'une justification (art. 6 RGPD) pour traiter des données personnelles.

Sur certains points, cependant, la nouvelle loi suisse sera plus stricte que le RGPD. Il s'agit notamment du champ d'application géographique (cf. point 3) et du champ d'application matériel (art. 2 nLPD). Selon la nLPD, ce dernier englobe tous les traitements de données (automatisés et manuels), alors que le RGPD ne s'applique qu'aux systèmes de fichiers pour ce qui concerne les traitements de données manuels. Ensuite, l'obligation d'informer de la collecte de données personnelles selon la nLPD va plus loin que le RGPD dans la mesure où, en cas de transmission de données à l'étranger, il faut informer sur tous les États destinataires (art. 19 nLPD). La nLPD prévoit également une obligation de journaliser le traitement de données automatisé et d'établir un règlement pour les traitements automatisés (art. 4 et 5 s. OPDo). De plus, sous la nLPD – à la différence du RGPD qui prévoit des amendes exclusivement pour les entreprises – des sanctions s'appliquent aux personnes physiques (art. 60 ss. nLPD) et, enfin, la notion de «données personnelles sensibles» comprend deux catégories supplémentaires: les poursuites et sanctions administratives ou pénales ainsi que des mesures d'aide sociale.

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 la taille d'une entreprise, elle possède nombre de données sur ses clients, partenaires, fournisseurs et collaborateurs. Avec la numérisation de l'économie, la quantité de données personnelles à traiter par les entreprises, PME comprises, ira d'ailleurs grandissant. Certaines des (nouvelles) obligations prévues par la nLPD dépendent toutefois de l'ampleur du traitement des données ainsi que du risque que le traitement comporte pour la personnalité ou les droits fondamentaux des personnes concernées. Cette approche fondée sur les risques, qui s'applique entre autres à la sécurité des données, permet de prendre des mesures au cas par cas. Toutefois, il va de soi que les PME peuvent aussi traiter des données personnelles sensibles à grande échelle ou exercer d'autres activités de traitement qui comportent un risque élevé pour la personnalité des personnes concernées.

Toutes les entreprises – y compris les PME – doivent se préparer de manière adéquate 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.

La seule «exception prévue pour les PME» concerne les obligations de tenir un registre des activités de traitement. Les PME employant moins de 250 personnes au 1er janvier sont exemptées de cette obligation, pour autant qu'elles ne traitent pas de «données personnelles sensibles» à grande échelle et qu'elles ne pratiquent pas de «profilage à risque élevé». Une entreprise a néanmoins intérêt à tenir un tel registre des activités de traitement sur une base volontaire, car celui-ci peut fournir une vue d'ensemble précieuse des traitements de données effectués dans l'entreprise et servir ainsi de fondement pour remplir d'autres obligations, telles que les obligations d'information vis-à-vis des personnes

concernées.

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

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

- l'obligation de mettre en place des mesures techniques et organisationnelles afin que le traitement des données respecte les prescriptions de protection des données dès la conception et 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) (cf. les nouveaux termes au point 12 ci-après);

- l'obligation d'effacer (ou d'anonymiser) les données personnelles qui ne sont plus nécessaires pour atteindre les objectifs poursuivis et qui ne sont pas soumises à une obligation légale de conservation est déjà en vigueur en vertu du principe de proportionnalité et désormais explicitement ancrée dans la loi (art. 6, al. 4, nLPD);

- l'obligation d'établir et tenir un registre des activités de traitement des données. Les entreprises de moins de 250 collaborateurs bénéficient ici d'une exception si leur traitement des données comporte un faible risque d'atteinte à la personnalité des personnes concernées (art. 12 nLPD et point 6 du présent document). L'OPDo précise qu'il existe un risque élevé lorsque des données personnelles sensibles sont traitées à grande échelle ou lorsqu'un profilage à risque élevé est effectué (art. 24);

- l'obligation de 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 et art. 15 OPDo). Contrairement au RGPD (qui prévoit un délai de 72 heures pour la notification), la nLPD ne fixe pas de délai explicite, mais indique que la notification doit être effectuée «dans les meilleurs délais». Le contenu obligatoire et la documentation sont réglés dans l'OPDo (art. 15);

- l'obligation d'effectuer au préalable une analyse d'impact relative à la protection des données lorsqu'il existe un risque élevé pour la personnalité ou les droits fondamentaux de la personne en raison du traitement de données (art. 22 nLPD et art. 14 OPDo);

- l'obligation d'informer lors de la collecte de données personnelles, que les données soient collectées directement auprès de la personne concernée ou auprès de tiers (art. 19 ss. nLPD et art. 13 OPDo). À noter que l'information relative à la collecte de données personnelles doit être simple et compréhensible pour les personnes concernées. Il convient d'en tenir compte, notamment en ce qui concerne l'élaboration de dispositions relatives à la protection des données. En ce qui concerne l'obligation d'information, la nLPD est plus stricte que le RGPD et c'est une exception (cf. aussi le point 5 ci-dessus). La violation (éventuellement) intentionnelle de cette obligation est sanctionnée par le droit pénal;

- l'obligation d'informer en cas de décision individuelle automatisée – c'est-à-dire une décision fondée exclusivement sur un traitement automatisé et

entraînant des conséquences juridiques pour la personne concernée ou l'affectant de manière significative (art. 21 nLPD). La violation (éventuellement) intentionnelle de cette obligation est sanctionnée par le droit pénal;

- l'obligation de journaliser le traitement automatisé de données personnelles sensibles à grande échelle ou le profilage à risque élevé lorsque les mesures préventives prises ne permettent pas de garantir la protection des données (art. 4 OPDo) ainsi que d'établir un règlement pour ces traitements automatisés et de le mettre à jour régulièrement (art. 5 OPDo).

8) Quels sont les nouveaux droits des personnes concernées?

La nouvelle réglementation vise principalement à renforcer la transparence et la protection des données personnelles des personnes concernées. Pour y parvenir, il faut notamment que les entreprises communiquent les informations sur la collecte de données personnelles de manière concise, compréhensible et facilement accessible (art. 13 OPDo) et que les droits de l'individu soient renforcés. Les droits de l'individu incluent par exemple:

- le droit d'être informé sur le 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 (art. 21 nLPD).

Certaines violations (potentiellement) intentionnelles du devoir d'informer sont passibles d'une sanction (art. 60 nLPD). Les entreprises devraient donc s'assurer qu'elles conservent à tout moment une vue d'ensemble des données personnelles qu'elles traitent et qu'elles peuvent répondre aux demandes des personnes concernées dans les délais et dans la forme requise.

9) Ai-je besoin d'une autorisation de la personne concernée pour pouvoir traiter ses données?

Non. Le traitement de données personnelles est autorisé aussi bien par le droit en vigueur que par le nouveau droit, tant qu'il n'y a pas d'atteinte illicite à la personnalité des personnes concernées. Il y a atteinte à la personnalité notamment lorsque:

- le traitement des données personnelles ne respecte pas les principes du traitement des données (art. 6 nLPD) et de la sécurité des données (art. 8 nLPD);
- des données personnelles sont traitées contrairement à la déclaration de volonté expresse de la personne concernée;
- des données personnelles sensibles sont communiquées à des tiers.

Contrairement au RGPD, un motif justificatif n'est en principe pas nécessaire (cf. aussi le point 5 ci-dessus). Selon la nLPD, le «principe d'autorisation avec réserve

d'objection» continue donc de s'appliquer, tandis que selon le RGPD, l'«interdiction de principe avec réserve d'autorisation» s'applique (art. 6 et 9 RGPD).

10) À quoi dois-je faire attention lorsque je fais appel à des prestataires externes qui traitent des données personnelles pour nous (fournisseurs de services cloud, prestataires de services RH, etc.)?

Les prestataires externes qui traitent des données personnelles pour le compte et sur instruction du mandant ou du «responsable» (cf. à ce sujet le point 12 ci-après), comme les fournisseurs de services cloud, les hébergeurs web, les services de gestion des salaires, etc. sont considérés comme des «sous-traitants» (art. 5, let. k nLPD).

Le traitement de données personnelles peut – comme c'est déjà le cas aujourd'hui – être confié par contrat ou par la loi à un sous-traitant si celui-ci traite les données comme le responsable serait lui-même en droit de le faire et si aucune obligation légale ou contractuelle de garder le secret n'interdit la délégation (art. 9 nLPD). Le recours à un sous-traitant présuppose donc en général un contrat (écrit) (convention de traitement de données par un sous-traitant ou CTD). Avant la délégation, le mandant ou le responsable doit s'assurer que le sous-traitant est en mesure de garantir la sécurité des données (art. 8 nLPD et art. 1 ss. OPDo). Le sous-traitant est légalement tenu d'obtenir l'autorisation préalable (générale ou spécifique) du responsable du traitement avant de faire appel à un tiers pour le traitement des données (art. 7 OPDo). Les parties peuvent inclure d'autres points dans la CTD (comme la procédure à suivre en cas de réclamation des personnes concernées ou de violation de la sécurité des données, les droits d'audit et de contrôle, la responsabilité, le for juridique, etc.) Dans la pratique, des contrats types fondés sur le contenu minimal selon le RGPD sont couramment utilisés.

Le fait de confier intentionnellement un traitement de données à un sous-traitant alors que les conditions prévues à l'art. 9, al. 1 et 2 ne sont pas remplies est punissable (art. 61, let. b nLPD).

11) Puis-je communiquer ou transmettre des données personnelles à l'étranger?

Par communication de données personnelles, on entend la «transmission ou la mise à disposition de données personnelles» (art. 5 let. b nLPD). Ainsi, la simple possibilité d'accès aux données par un organisme à l'étranger (équipe d'assistance, par exemple) constitue également une communication au sens de la nLPD.

La communication de données personnelles à l'étranger est autorisée dans la mesure où l'État destinataire dispose d'une législation garantissant un niveau de protection des données «adéquat» (art. 16, al. 1 nLPD). Les États qui remplissent cette condition sont définis par le Conseil fédéral et publiés dans l'annexe 1 de l'ordonnance sur la protection des données.

Inversement, cela signifie que tous les États qui ne figurent pas sur cette liste ne disposent pas d'un niveau de protection des données «adéquat» et qu'il n'est donc possible de communiquer des données personnelles qu'en mettant en place des

mesures de protection supplémentaires (art. 16, al. 2 et art. 17 nLPD ainsi qu'art. 9 OPDo). Les clauses types de protection des données (SCC) sont utilisées à cette fin. L'exportateur de données doit s'assurer par des mesures appropriées que le destinataire des données respecte les SCC (art. 10 OPDo). Étant donné que les SCC ne lient que le destinataire en tant que partie contractante, mais pas les autorités locales, et que les données personnelles transférées ne sont donc pas protégées contre tout accès par un État, l'exportateur de données doit préalablement évaluer le risque d'accès inacceptable du point de vue suisse par les autorités en procédant à un «Transfer Risk Assessment» (TIA) (clause 14 SCC). Selon le risque, il convient de prendre des mesures de protection supplémentaires (pseudonymisation, cryptage des données, par exemple) ou de renoncer totalement au transfert de données.

La violation (potentiellement) intentionnelle des dispositions relatives à la communication de données personnelles à l'étranger est passible de sanctions (art. 61, let. a nLPD).

En ce qui concerne la communication de données personnelles aux États-Unis, nous attirons l'attention sur le nouveau cadre UE-États-Unis de protection des données personnelles (Data Privacy Framework ou DPF), qui permet aux entreprises américaines de se faire certifier en tant qu'importateurs de données. Depuis la décision d'adéquation de la Commission européenne du 10 juillet 2023, les transferts de données de l'UE vers des entreprises américaines certifiées dans le cadre du Data Privacy Framework sont considérés comme des transferts de données vers un pays offrant un niveau «adéquat» de protection des données (cf. communiqué de presse). On peut s'attendre à ce que le PFPDT établisse prochainement le niveau de protection adéquat pour la Suisse (CH-US Data Privacy Framework) des transferts de données dans ce cadre.

12) Quels nouveaux termes sont importants pour comprendre le droit de la protection des données?

La nouvelle loi sur la protection des données a introduit quelques nouveaux termes ou les a partiellement harmonisés avec le RGPD. Les plus importantes sont:

- Données personnelles: Le terme ne s'applique qu'aux personnes physiques. Les données relatives aux personnes morales ne sont donc plus concernées et sont par conséquent exclues du champ de protection de la LPD (art. 1 et art. 5, let. a nLPD).
- Données personnelles sensibles: Sont désormais également concernées les données relatives à l'appartenance à une ethnie, les données génétiques et les données biométriques (permettant une identification univoque) (art. 5, let. c nLPD).
- Responsable du traitement: Correspond au «maître du fichier» selon le droit en vigueur et au «responsable du traitement» selon le RGPD. Il s'agit d'une personne privée (en particulier d'une entreprise) ou d'un organe fédéral qui, seul ou avec d'autres, décide des finalités et des moyens du traitement de données personnelles (art. 5, let. j nLPD). Par exemple, un employeur qui traite les données personnelles de ses employés dans le cadre de l'exécution du contrat de travail ou un commerçant qui traite les données personnelles de ses clients dans le cadre de l'exécution du

contrat de vente.

- Sous-traitant de données: Est considérée comme sous-traitant toute personne qui traite des données personnelles pour le compte du responsable, par exemple les prestataires de services cloud (art. 5 let. k nLPD, cf. point 10 ci-dessus).
- Profilage: Ce terme désigne toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la localisation, par exemple). Des conséquences juridiques plus sévères ne s'appliquent toutefois qu'au «profilage à risque élevé», qui comporte un risque marqué 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. Le profilage à risque élevé est comparable au concept actuel de «profil de la personnalité». À noter que la nLPD n'introduit pas d'exigence de consentement pour le profilage à risque élevé, mais se contente d'exiger que le consentement, s'il devait être requis comme motif justificatif en vertu de l'art. 31 nLPD, soit «explicite». Dans ce contexte, il convient de rappeler que le traitement de données personnelles ne requiert en principe aucun motif justificatif, que ce soit dans le cadre du droit en vigueur ou du nouveau droit (cf. points 5 et 9 ci-dessus).
- Principes de «Privacy by Design» et de «Privacy by Default»: La nLPD introduit les principes de «Privacy by Design» et de «Privacy by Default». Comme son nom l'indique, le principe de «Privacy by Design» (respect du principe de protection des données dès la conception) signifie que des mesures techniques et organisationnelles doivent être prises dès la planification d'un système de traitement, notamment pour garantir la sécurité des données personnelles. Le principe de «Privacy by Default» (protection des données par défaut) signifie que les paramètres par défaut d'un système de traitement des données doivent être configurés de manière que seules les données personnelles qui sont effectivement nécessaires pour l'objectif de traitement déterminé soient traitées. Cette disposition vise à protéger les utilisateurs n'ayant pas d'affinités avec la technique qui ne savent pas comment modifier eux-mêmes les paramètres de protection des données en fonction de leurs préférences. Il convient de noter qu'il est nécessaire de procéder à un paramétrage préalable favorable à la protection des données exclusivement dans les cas où les paramètres peuvent être modifiés.

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

En cas de violation de la nouvelle loi, vous vous exposez à des sanctions sous forme d'amendes pouvant aller jusqu'à 250 000 francs (si vous ne respectez pas vos obligations d'information ou de renseignement, par exemple – art. 19 ss. et 25 ss. nLPD) ou votre devoir de diligence, notamment en communiquant illégalement des données personnelles à l'étranger (art. 16 s. nLPD) ou à un sous-traitant (art. 9 nLPD) ou si vous ne respectez pas les exigences minimales en matière de sécurité des données (art. 8 nLPD en relation avec l'art. 1 s. OPDo). Contrairement

au RGPD, les sanctions prévues par la nLPD ne sont pas dirigées contre l'entreprise fautive, mais contre la personne physique responsable du respect de la protection des données (le directeur ou le membre du conseil d'administration, mais aussi, dans certaines circonstances, d'autres collaborateurs, par exemple). Seul un comportement (potentiellement) intentionnel est sanctionné (art. 60 ss. nLPD). Exceptionnellement, les entreprises peuvent aussi être directement mises en cause si une amende de 50 000 francs au maximum est envisagée et si l'identification de la personne physique coupable au sein de l'entreprise ou de l'organisation entraînerait des frais d'enquête disproportionnés (art. 64, al. 2 nLPD).

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 pour sa réputation. Les compétences du Préposé fédéral à la protection des données (PFPDT) ont également été élargies (art. 51 nLPD). Désormais, il peut non seulement émettre des recommandations, mais aussi ordonner des mesures administratives (ordonner l'adaptation, l'interruption ou l'annulation d'un traitement ou l'effacement de données personnelles, par exemple), ce qui peut constituer une mesure drastique pour certaines entreprises.

14) Comment se préparer aux changements?

Il est tout d'abord nécessaire de s'y préparer dès que possible à l'aide d'une analyse des lacunes existantes afin d'adapter graduellement la conformité en matière de protection des données à ce nouveau régime réglementaire. Selon la taille de l'entreprise et l'ampleur des traitements de données, ce processus peut prendre quelques jours ou plusieurs mois. Pour les entreprises qui sont déjà en conformité avec le RGPD, la tâche sera bien entendu plus simple que pour celles qui commencent tout juste. 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, contrats de sous-traitant, transferts de données vers des pays tiers, etc.).

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 élaboré une charte de l'économie suisse pour une gestion responsable des données. Si cela se révèle nécessaire faute d'expertise et/ou de ressources internes, les entreprises devraient faire appel à des experts en sécurité informatique et en protection des données, que ce soit pour l'élaboration ou des vérifications ponctuelles de documents (déclarations de protection des données, par exemple) ou de contrats (CTD), ou pour l'élaboration de programmes de conformité détaillés (directives, processus, par exemple).

15) Que doit-on faire pour se mettre en conformité? Quelles actions sont requises?

Sans entrer dans des aspects techniques, juridiques et informatiques détaillés d'une mise en conformité avec la nLPD, un plan d'action pragmatique devrait au moins retenir les mesures suivantes:

1. **Définir les responsabilités et les fonctions**
   Eu égard à la planification, il est important de commencer par définir les responsabilités et d'attribuer des fonctions. Il est judicieux de créer un service central de protection des données (coordinateur, personne de contact).

   Dans ce contexte, il est possible d'examiner rapidement s'il faut désigner un conseiller à la protection des données (contrairement au RGPD, la nLPD prévoit que cela est facultatif pour les privés – seuls les organes fédéraux en ont l'obligation légale, art. 10 nLPD et art. 23 OPDo).

2. **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. (art. 19 ss. nLPD et art. 13 OPDo). 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 (art. 25 ss. nLPD et art. 16 ss. OPDo). 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 (registre dit des activités de traitement) peut servir de point de départ. Cela permet non seulement de créer une bonne base pour élaborer d'autres documents (obligatoires) relatifs à la protection des données (dispositions relatives à la protection des données, sous-traitance, etc.), mais également d'assumer en même temps l'obligation (éventuelle) de tenir un registre des activités de traitement. Un tel état des lieux est un effort collectif de tous les collaborateurs impliqués dans le traitement de données personnelles.

3. **Analyse des lacunes et évaluation des risques**
   Les travaux nécessaires pour la mise en conformité peuvent être identifiés puis documentés au moyen d'une analyse des lacunes (comparaison de l'état actuel et de l'objectif à atteindre). Pour cela, il est également possible de recourir à des modèles de registre des activités de traitement.

   Certaines obligations de la nLPD, comme les exigences en matière de sécurité des données, l'obligation pour les PME de tenir des registres des activités de traitement ou l'obligation de réaliser une analyse d'impact sur la protection des données, dépendent du risque que présentent le traitement de données au sein de l'entreprise. Aussi une évaluation préalable des risques est-elle nécessaire pour déterminer les mesures concrètes en vue de la mise en œuvre. Pour garantir une sécurité des données adéquate, il convient de déterminer le besoin de protection des données personnelles et de définir les mesures techniques et organisationnelles appropriées au regard du risque. Pour les critères permettant de déterminer le besoin de protection des données

personnelles, on peut se fonder sur les critères de l'art. 1, al. 2 OPDo et pour ceux permettant d'évaluer le risque pour la personnalité ou les droits fondamentaux de la personne concernée sur les critères de l'art. 1, al. 3 OPDo. Au moment de définir des mesures techniques et organisationnelles, il convient en outre de tenir compte de l'état de la technique et des coûts de mise en œuvre (art. 1, al. 4 OPDo).

Des risques accrus et donc des exigences plus élevées en matière de conformité à la réglementation en matière de protection des données (en particulier la sécurité des données) peuvent exister, 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, let. c 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, etc. sont concernées.
- Les entreprises effectuent un profilage à risque élevé.
- Les entreprises prennent des décisions individuelles automatisées.

Dans ces cas, les exigences relatives à la protection des données et en particulier à la sécurité des données sont plus élevées 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, régulièrement, l'établissement de processus 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.

4. **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.

   Ni la nLPD ni le RGPD n'exigent explicitement l'organisation de formations,

mais dans les faits, celles-ci sont souvent nécessaires (et peuvent éventuellement avoir pour effet de réduire la responsabilité en cas d'infraction pénale) afin de créer la sensibilité nécessaire à ce sujet dans l'entreprise.

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.

5. **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).

6. **Sécurité informatique**
   En ce qui concerne la sécurité des données, les entreprises doivent s'assurer que la sécurité des systèmes informatiques de l'entreprise et des applications logicielles répondent aux exigences de la nouvelle loi. Cela comprend des mesures techniques et organisationnelles (établir des droits d'accès, pseudonymiser des données, etc.) visant à prévenir les cyberattaques, la manipulation et le vol de données ainsi que d'autres pertes de données. Avec ces mesures, il s'agit de tendre vers les objectifs de protection de la sécurité des données selon l'art. 2 OPDo (confidentialité, disponibilité, intégrité et traçabilité).

   Dans ce contexte, il convient 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 (art. 61, let. c nLPD).

7. **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 claires ainsi que des règlements ou des directives y relatifs. Selon l'incident, ceux-ci doivent définir en particulier quel(s) collaborateur(s) (suppléants inclus) doi(ven)t 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).

8. **Établir et tenir 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 et art. 24 OPDo).

   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.

9. **Révision des contrats**
   Au vu des changements qui s'opéreront avec la nouvelle loi et d'ici à 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 à leur tour des contrats – ou une adaptation des contrats déjà existants – incluant des clauses conformes à la nouvelle loi sur la protection des données.

10. **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 procédures 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 les Chambres de commerce, par exemple).

    Il convient de noter que garantir la conformité en matière de protection des données n'est pas un exercice ponctuel. Au contraire, celle-ci doit être contrôlée régulièrement et, si nécessaire, adaptée, notamment au vu des évolutions techniques (nouveaux systèmes informatiques, par exemple), juridiques (adaptations législatives ou de la pratique des autorités, par exemple) et entrepreneuriales (nouveaux services, nouvelles succursales dans d'autres pays, par exemple). En ce qui concerne la sécurité des données, l'art. 1, al. 5, OPDo prescrit explicitement que le besoin de protection des données personnelles, le risque encouru ainsi que les mesures techniques et organisationnelles doivent être réévalués pendant toute la durée du traitement et adaptés en cas de besoin. Il importe d'établir les procédures et les responsabilités pour ces vérifications.