allnews La finance suisse dans l'e-media

Protection des données personnelles: nouveautés et mise en œuvre

1 mai 2023 - 07:00

| Véronique Chatelain Gomez, FBT Avocats

4 minutes de lecture

Le Conseil fédéral a xé en août 2022 l'entrée en vigueur de la Loi révisée sur la protection des données («nLPD») et de ses ordonnances d'application au 1er septembre 2023.

Le droit suisse de la protection des données a fait l'objet d'une révision intégrale rendue nécessaire notamment par le développement continuel des nouvelles technologies et des réseaux sociaux. L'objectif est de renforcer la protection de toute personne concernée par le traitement de ses données personnelles en améliorant, d'une part, la transparence relative à ce traitement et, d'autre part, le droit d'accès à ses données, mais également de maintenir la compatibilité du droit suisse avec le droit européen et préserver ainsi la libre circulation des données, tout en garantissant la compétitivité de la Suisse. Adoptée à l'automne 2020 par le Parlement, le Conseil fédéral a xé en août 2022 l'entrée en vigueur de la Loi révisée sur la protection des données («nLPD») et de ses ordonnances d'application au 1er septembre 2023, laissant ainsi aux responsables de traitement (anciennement «maîtres de chier») une année pour se conformer aux nouvelles dispositions.

Nous nous limiterons ici à présenter quelques-unes des nouveautés qui affectent les personnes et entités privées responsables du traitement des données et à proposer certaines démarches à entreprendre en vue d'une mise en conformité. Ces démarches pourront varier

selon le type de traitement des données et le risque d'une atteinte élevée à la personnalité ou aux droits fondamentaux de la personne concernée, mais également selon la taille de l'entreprise ou selon que celle-ci a dû se conformer au Règlement européen sur la protection des données en 2018. Au nombre des premières étapes figurent l'analyse des mesures techniques et organisationnelles pour la sécurité des données, la révision, voire, selon les circonstances, la rédaction de directives en matière de traitement des données, ou encore l'analyse des contrats avec les sous-traitants sous l'angle de la protection des données.

L'on peut évoquer:

- la limitation du champ d'application de la nLPD aux données de personnes physiques, alignant ainsi le droit suisse au droit européen et à la majorité des législations étrangères; les données de personnes morales restent néanmoins protégées par d'autres dispositions du droit suisse (comme les articles 28 ss CC sur la protection de la personnalité ou le droit sur la concurrence déloyale);
- l'extension de la définition des données sensibles aux données génétiques et biométriques (par exemple, empreintes digitales ou vocales) dès lors que celles-ci permettent l'identification d'une personne;
- l'introduction de la notion de profilage (soit le traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser sa situation économique) en lieu et place de celle de profil (consistant en l'assemblage de données permettant d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique);
- l'introduction des principes de privacy by design et de privacy by default: à l'avenir, la protection des données et le respect de la vie privée des utilisateurs doivent être intégrés dans la structure même du produit ou du service dès sa conception. Par ailleurs, le niveau de sécurité le plus élevé doit être garanti dès la mise en circulation du produit ou du service par l'activation par défaut de toutes les mesures techniques et organisationnelles nécessaires à la protection des données et à la limitation de leur utilisation;
- la désignation d'un conseiller à la protection des données qui aura pour tâches principales la fourniture de conseils et la formation du personnel et qui assistera également à l'élaboration et à l'application de conditions d'utilisation et de dispositions en matière de protection des données. Il convient de relever que la désignation d'un tel conseiller reste facultative pour les personnes et entités privées, contrairement à ce que prévoit le droit européen. L'opportunité de désigner un tel conseiller doit toutefois être évaluée;
- l'obligation de procéder à des analyses d'impact, jusqu'alors obligatoires pour les organes fédéraux seulement, est étendue aux personnes privées; ces analyses ne sont obligatoires qu'en cas de traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées, avec la possibilité d'y renoncer en cas de certification au sens de la nLPD (nouvellement introduite en droit suisse) d'un système, d'un produit ou d'un service, ou de respect du code de conduite d'une association professionnelle, sectorielle ou économique reposant lui-même sur une analyse d'impact. La nLPD encourage les milieux intéressés à rédiger un code de conduite et à le soumettre, s'ils le souhaitent, au Préposé fédéral à la protection des données et à la transparence (PFPDT) pour qu'il prenne position sur ses dispositions. Un avis favorable de sa part permet de présumer qu'un comportement défini dans le code respecte la protection des données;
- le renforcement des devoirs d'information (qui peut être standardisé) et d'accès aux données personnelles par les personnes concernées: l'obligation d'informer – en principe au moment de la collecte de données – s'applique dorénavant à tout responsable de traitement et à tout traitement, quelles que soient les données. Le responsable de traitement est tenu de communiquer à la personne concernée les informations nécessaires afin qu'elle puisse faire valoir ses droits. Toute entreprise doit permettre à une personne concernée de demander et recevoir ses données sous format électronique. Il convient de

noter également, en cas de communication des données vers l'étranger, que l'obligation d'informer doit mentionner les pays vers lesquels les données sont transférées et le niveau de protection offert ou la mise en place de garanties. La liste des pays offrant un niveau de protection adéquat figure dorénavant dans la nLPD;

Les entreprises doivent donc revoir, le cas échéant, adapter, leur déclaration en matière de protection des données, laquelle peut figurer dans leurs conditions générales ou sur leur site internet. Elles doivent également revoir les pays vers lesquels les données sont transmises (en cas, par exemple, de stockage sur un cloud). Il convient enfin de prévoir une marche à suivre pour répondre rapidement aux demandes de renseignement et de suppression des données;

- la tenue, avec mise à jour régulière, d'un registre des activités de traitement, dont la nLPD précise le contenu. Les entreprises comptant moins de 250 employés et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées sont exemptées. Le traitement en question ne doit pas porter sur des données sensibles (par exemple, les données sur les opinions politiques, sur la santé, les données biométriques, les données relatives aux poursuites ou sanctions pénales et administratives) à grande échelle ni constituer un profilage à risque élevé. Pour les entreprises exemptées, l'opportunité de tenir un tel registre devrait toutefois être analysée;
- l'introduction de l'obligation d'annoncer rapidement au PFPDT toute violation de la sécurité des données ayant pour conséquence vraisemblable un risque élevé pour la personnalité ou les droits fondamentaux de la personne. Les assujettis à la Finma connaissent déjà un tel devoir d'annonce en cas de cyberattaques. Le devoir d'annonce est donc étendu, puisqu'il s'agit d'effectuer également une annonce auprès du PFPDT qui portera sur toute violation de la sécurité comportant un risque élevé d'atteinte à la personnalité. Il convient donc de mettre en place ou de revoir la procédure dite de «signalement».

Si la nLPD n'apporte pas de changements majeurs aux principes fondamentaux au cœur de la protection des données (licéité du traitement, proportionnalité, finalités reconnaissables et déterminées, exactitude, consentement, sécurité et destruction des données qui ne sont plus nécessaires), elle les renforce en introduisant de nouvelles obligations dont la violation peut comporter des sanctions pénales. La nLPD ne prévoit pas de période transitoire en raison du délai d'un an avant son entrée en vigueur. Le 1er septembre 2023, les entreprises suisses devront s'être conformées au nouveau droit de la protection des données.

Véronique Chatelain Gomez
Collaboratrice

Véronique Chatelain Gomez est collaboratrice et membre des groupes bancaire et financier et du droit patrimonial de la famille de FBT. Elle conseille des établissements bancaires suisses et étrangers, des sociétés actives dans la gestion de fortune collective et individuelle, et des distributeurs. Elle s'intéresse en particulier aux questions liées à la surveillance et à la lutte contre le blanchiment d'argent.

FBT
AVOCATS

FBT Avocats SA est une Etude pluridisciplinaire, implantée à Genève et à Paris, qui intervient dans des activités de niches, à dominante transfrontalière. FBT Avocats SA est l'une des Etudes les plus spécialisées en droit bancaire et financier de Suisse romande. Elle couvre par ailleurs le droit patrimonial de la famille, le droit des sociétés, le droit du travail et des assurances sociales, le contentieux civil, administratif et pénal et la fiscalité.