Entrée en vigueur de la nouvelle LPD : enjeux et recommandations

Cette fois, ça y est, plus personne n'est censé ignorer l'entrée en vigueur de la nouvelle LPD le 1er septembre 2023.

Dans le cercle restreint, toutefois, des acteurs de la protection des données et des organismes confrontés de près à ces problématiques. Car on ne peut pas dire que le Préposé fédéral nous envahisse d'information ou d'émissions à ce sujet.

S'agissant des bases, je rappelle que toute donnée personnelle – à savoir toute information relative à une personne identifiée ou identifiable – doit être traitée, de la collecte à la suppression en passant par la modification, la communication, l'exploitation, la conservation, en application des sept principes que sont la licéité, la finalité, la proportionnalité, la bonne foi et la transparence, l'exactitude et la sécurité, et que toute personne a le droit d'accès à ses données personnelles.

Quelles sont les nouveautés ?

En plus de modifications terminologiques ou cosmétiques et de certaines précisions, sont renforcés les droits de la personne concernée, les compétences des autorités de surveillance et les responsabilités des acteurs principaux que sont le Responsable de traitement et le sous-traitant. On pourrait résumer cela en disant que désormais il convient d'être clair et complet sur la communication que l'on fait aux personnes concernées pour tout type de traitement, et que le sous-traitant, coresponsable de la conformité en particulier de la sécurité des données si l'on songe à l'hébergeur, doit collaborer avec le responsable de traitement pour permettre à celui-ci de remplir ses missions légales, en particulier s'agissant du droit d'accès mais aussi de la violation des données.

Les obligations nouvelles sont, en effet, d'une part l'obligation pour tout responsable de traitement d'annoncer la violation des données - en n'oubliant pas que l'on entend par là non seulement les intrusions dans un système d'information sécurisé mais également la perte d'un matériel contenant des données personnelles ou encore l'accès illégitime à des données personnelles. D'autre part, l'obligation de faire une analyse d'impact dans les situations ou projets dont on peut pressentir un impact important sur le droit des personnes concernées – qu'il s'agisse d'un gros volume de données personnelles traitées ou de données personnelles sensibles.

Une nouvelle obligation est celle qui concerne le représentant en Suisse, pour les entreprises de l'union européenne qui cible la Suisse et donc qui se verront appliquer la LPD. Il s'agit-là du pendant de l'obligation inverse : l'entreprise suisse qui cible le territoire de l'union doit en effet avoir un représentant sur ce territoire.

On trouvera également dans la nouvelle LPD le concept de Protection dès la conception et par défaut, qui en tant que tel est nouveau, mais, à l'instar de cette obligation prévue par le RGPD, revient uniquement à exiger du responsable de traitement qu'il s'assure de la conformité du traitement sous l'angle des sept principes, évidemment avant de mettre un produit sur le marché (dès la conception) et à le paramétrer de manière à garantir un traitement conforme (par défaut).

Alors on peut dire, à l'instar de certaines entreprises, vendeuses de produits, que les nouveautés de la LPD sont nombreuses, cela ayant au moins pour effet de motiver les troupes. Pour ma part, je considère que l'enjeu principal est d'être en conformité par rapport aux sept principes rappelés ci-dessus, qui existent depuis 1993.

Que faire alors et par quoi commencer ? La conformité en protection des données commande avant tout que l'on accepte de revoir ses processus, de se questionner sur ce dont on a besoin pour

atteindre tel objectif, et rien de tel qu'une formation pour mettre tout le monde à niveau, et faire émerger, à l'interne, de l'intérêt pour la matière. Des référents internes, sensibilisés à la protection des données et qui se forment régulièrement et se confrontent aux difficultés, c'est le meilleur garant de la conformité.

Ne pas oublier de revoir également la documentation existante, pour voir s'il convient de la compléter, de la mettre à jour, je pense en particulier aux contrats qui nous lie à nos fournisseurs et prestataires.

Et puis recenser les traitements. Certes, en raison des lobbys fédéraux l'obligation ancrée dans la nouvelle loi de tenir un registre des traitements a été réduite à peau de chagrin par l'ordonnance, qui prévoit une exception pour les organisations de moins de 250 salariés, ce qui, vu le tissu économique suisse essentiellement constitué de PME revient quasiment à la suppression de cette obligation. Mais tous les acteurs de la protection des données vous le diront : impossible de faire de la conformité sans avoir préalablement recensé et décrit les différents traitements. Vive le registre des traitements, par conséquent !

ID 26.01.2023